Risk Methodology K-12

Prepared by
Carol Woody, Ph. D.

Based on the Operationally Critical Threat, Asset, and Vulnerability Evaluation [SM]

NOTE: This methodology was developed to support the dissertation **Applying Security Risk Management to Internet Connectivity in K-12 Schools and School Districts** in partial fulfillment of a requirements for a Ph. D. in Information Systems, Graduate School of Computer and Information Sciences, NOVA Southeastern University (2004)

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University

K-12 Risk Methodology Introduction

Technology is broadly used in the K-12 environment by many participants including administrators, teachers, parents, students, school board members, community officials and tax payers. While this enables a wide range of useful activities, the risk for inappropriate and illegal behavior that violates privacy, regulations, and common courtesy is increasing exponentially. A methodology called OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation) was released in 2001 by the Software Engineering Institute at Carnegie Mellon University to assist large organizations in planning for and mitigating cyber-security and other technology related risks. In April 2004 this version of OCTAVE tailored for K-12 schools and school districts became publicly available. This document provides detail guidance and worksheets for you to apply the K-12 Risk Methodology within your institution to construct a plan to help your organization reduce cyber-related risk.

For those familiar with the OCTAVE Methodology, the following tailoring options were applied to create a version applicable to K-12:

- Expanded catalog of practices assembled from threats and practices based on threats and mitigation activities identified from media incidents
- Expanded survey and protection strategy templates to incorporate the expanded catalog
- Modified evaluation criteria to included options needed for K-12
- Data gathering steps were modified to collect information from within the analysis team and only optionally from other sources

This methodology was piloted by the Scarsdale School District, Scarsdale, NY. In addition, the methodology was reviewed by members of the Consortium for School Networking (www.cosn.org) for reasonability and applicability to K-12 schools and school districts.

Getting Started

Select an analysis team (3-5 participants) to perform the methodology and develop a plan. This team should include representatives from each of the major technology user groups (e.g. teaching, curriculum development, administration) and IT support. The analysis team will use the guidance and worksheets to develop a plan for identifying important information assets, threats to those assets, and steps for reducing the risk that these threats will materialize.

This methodology is designed to be self-administered. The participants will use the guidance and worksheets through a series of team discussions (workshops) grouped into three phases to assemble a plan. One member of the analysis team must gain familiarity with the methodology and concepts of operational security risk management to coordinate the team and keep the effort

Value of Using the K-12 Risk Methodology

The security focused conversations among members of the analysis team provide a forum for information sharing that is critical to reducing cyber-security risk, but does not happen in the course

---

® OCTAVE is registered in the United States Patent and Trademark Office by Carnegie Mellon University

of normal work. The structure of the methodology forces team members to discuss and analyze questions about cyber-security as a group. The knowledge level of all participants is increased based on this sharing mechanism. Viewing multiple perspectives gives the team confidence in the planned outcomes.

It is imperative that the team commit to complete the full risk methodology before attempting to implement solutions. Based on use by the pilot site, many initial ideas were generated during Phase 1 but these would not have addressed the major risks to the school district and addressing them would have taken resources away from completing the methodology. All three phases must be completed to assemble an effective plan for the institution.

This methodology does not focus on specific technology products and can be applied to every type of infrastructure.

How the Pilot Group Applied the Methodology

Project Kick-off Meeting

At the initial meeting of the analysis team, the following topic areas were discussed:

- Hardware, software, network infrastructure components and services that compose the infrastructure and the technical support available from a system administration perspective;
- Security policy, procedures, practices, monitoring efforts, and problems; and
- Distinctive features of the school district that makes technology important and vulnerable.

The value of using the risk assessment was analyzed and expected benefits defined. This session was facilitated by a security professional familiar with the security risk methodology.

Critical Asset Selection

One asset was selected from each group participating in the analysis team. This forced each group to seriously consider the security within their area. Instructional technology, administrative systems, and IT were represented on the analysis team. The student folder repository, payroll database, and ISP Internet connection were selected as assets.

Areas of Concern and Threat Identification

The analysis team had difficulty identifying threats that had not actually materialized. The normal mode of operation for the participations was reactive. To think in a proactive mode, the sequence of steps was changed and creation of evaluation criteria (Phase 3 – A3.2) was performed before proceeding with identifying threats to critical assets (Phase 1 – A1.6).

Instead of creating areas of concern then attempting to map them to the threat trees, the analysis team had each asset owner complete a set threat trees for their specific asset by assuming all branches on the trees were equally likely and determining if the impact would be high, medium, or low based on evaluation criteria. These impacts were discussed as a group and adjusted based on input from other analysis team members.

Creation of Evaluation Criteria

The analysis team adjusted the criteria areas to be the following:

- Required by regulatory mandate
- Led to an article on the front page of the local newspaper
- Resulted in parents calling members of the school board with complaints
- Affected the ability of teachers and students to meet their classroom schedules, and
- Interrupted online services especially Internet access.

Because the functions of the school district are so highly dependent on electronic communications, the loss of online services was identified as the most critical impact and could be used to evaluate all potential threats. The analysis team assigned the following levels of impact:

- A low impact would involve up to a half-day interruption
- A medium impact would involve up to two days of interruption
- A high impact would involve anything over two days.

Phase 2: Technology View

The analysis team did not have the required expertise to perform the vulnerability assessment within the required timeframe. They decided to identify this as a need for the future and proceed with the remainder of the assessment.

Additional Notes

Many good ideas were generated through the discussions of the survey results (Phase 1 – A1.5). Actions identified during these discussions should be captured for later consideration.

Schedule workshop sessions as close together as possible. The work can be broken into many manageable chunks, but if there is too much delay between gatherings a great deal of relearning must occur at each session. Assemble worksheets and notes from each workshop for distribution to all participants. When meetings have to be delayed or someone misses a session, this maintains an important level of continuity.

K-12 Methodology Contents

This booklet is divided into five major parts:

- Phase 1 Guidance: Organizational View (G1)
- Phase 2 Guidance: Technological View (G2)
- Phase 3 Guidance: Strategy and Plan Development (G3)
- Worksheets (w)
- Asset Profile Workbook - worksheets specific to selected critical assets (APW)

Reference Material

The examples and guidance for the OCTAVE Methodology, from which the K-12 Risk Methodology was derived, can help the analysis team in using the K-12 Risk Methodology. This information is available at www.cert.org/octave.

The authors of the OCTAVE Methodology (Christopher Alberts and Audrey Dorofee) published a book, Managing Information Security Risk (Addison-Wesley, 2003), which provides further examples and more detailed explanations to aid the analysis team in this effort.

Risk Methodology K-12

Phase 1 Guidance: Organizational View

During Phase I

Activity		Description	Worksheets
A1.1	Identify Assets and Relative Priorities	Identify assets that are used by the organization. They then select the most important assets to the organization and discuss their rationale for selecting those assets.	*Asset* worksheet (W1.1)
A1.2	Select Critical Assets	Identify assets that can have a large adverse impact on the organization if harmed.	*Asset Profile Workbook* (one for each critical asset)
A1.3	Identify Areas of Concern	Identify scenarios that threaten their most important assets based on typical sources and outcomes of threats. Consider impacts to the organization for their scenarios.	*Areas of Concern* worksheet (W1.2) *Asset Profile Workbook*
A1.4	Identify Security Requirements for Most Important Assets	Identify the security requirements for their most important assets. Select the most important security requirement for each important asset.	*Asset Profile Workbook*
A1.5	Current Protection Strategy Practices and Organizational Vulnerabilities	Complete surveys to indicate which practices are currently followed by the organization's personnel as well as which are not followed. After completing the survey, discuss specific issues from the survey in more detail.	*Current General Security Practices Survey* (W1.3) *Current Educational Security Survey* (W1.4) *Current IT Security Practices Survey* (W1.5) *Protection Strategy* worksheet (W1.6) *Security Practices Summary* (W1.7)
A1.6	Identify threats to critical assets	Threats are identified from areas of concern mapped to structured profiles.	*Asset Profile Workbook*
A1.7	Identify Evaluation Criteria	The organization uses evaluation criteria for all activities. These must be identified and applied to security.	*Identify Evaluation Criteria* (W1.8)

A1.1	**Identify Assets and Relative Priorities**	
Worksheets Used in this Activity	**Outputs of this Activity**	**Training**
• *Asset* worksheet (W1.1)	• important assets with relative priorities	Select one asset

Basic Guidance

An asset is something of value to the organization. An information security risk evaluation is focused on identifying the information that is important to meeting the mission of the organization. For each key function of the organization (teaching, learning, administration) identify the information assets that are needed to perform and support the critical activities within each function.

1. Identify key assets.

   Assets can fall into the following categories:

   - information – documented (paper or electronic) information or intellectual assets used to meet the mission of the organization
   - systems – information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered a system.
   - software and services – software applications (operating systems, database applications, networking software, office applications, custom applications, etc.)
   - hardware – information technology physical devices (workstations, servers, etc.)
   - people – the people in the organization, including their skills, training, knowledge, and experience

2. Complete the *Asset* worksheet (W1.1). Discuss each question on the worksheet. The following questions will be covered:

   - What are your important assets?
   - Are there any other assets that you are required to protect (e.g., by law or regulation)?
   - What related assets are important?
   - From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?

A1.1 Identify Assets and Relative Priorities

Additional Guidance

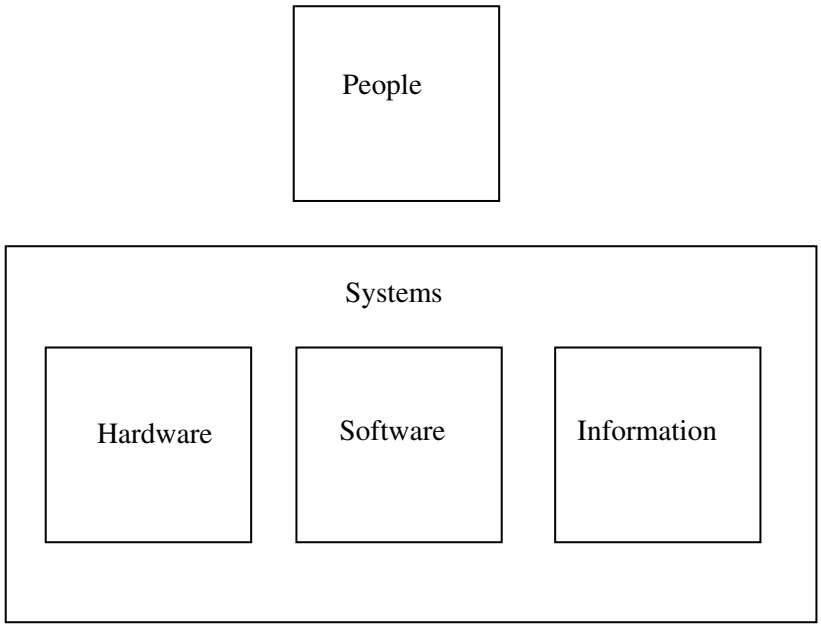
Clear definitions of assets are critical to effective security analysis.

Systems assets constitute the broadest of the asset categories, representing a grouping of information, software, and hardware assets. Most people think of a system as a whole; they don't break it down into its components. Because of this, systems assets are often identified during an information security risk evaluation.

Information assets are intangible in nature and are closely linked to systems assets. Systems store, process, and transmit the critical information that drives organizations. Thus, when an organization creates strategies and plans to protect its systems assets, it is also protecting its critical information (as well as its software and hardware assets). Don't forget that some information assets are represented physically (on paper).

When people identify *software assets*, you should try to determine whether they are referring to software applications or services, or whether they are actually referring to systems. For example, when someone identifies a software application, such as a database application, you should determine whether he or she believes that the software or the database system is the important asset. In many cases, the person will be looking at the asset more broadly and will be referring to the database system (which includes the information). In another example, the participants might identify office automation software (word processing applications, spreadsheet applications, etc.) as assets. Here, they are likely to be referring to the applications, not to systems. Use your best judgment when refining the list of assets.

Likewise, when people identify *hardware assets*, you should try to determine whether they are referring to physical hardware are actually referring to systems. For example, if someone identified personal computers as an asset, you should determine whether he or she believes that the PC hardware or the PC host (system) is the important asset. In many cases, you'll find that the person will be referring to the PC as a systems asset.



A1.2 **Select Critical Assets**

Worksheets Used in this Activity	Outputs of this Activity	Training
• *Asset Profile Workbook* for each critical asset	• critical assets (consider one asset of each type)	

Basic Guidance

Critical assets are those that are believed to be the most important assets to the organization. The organization will suffer a large adverse impact if the security requirements of these assets are violated.

1. Consider the following questions when selecting critical assets:
    - Which assets will have a large adverse impact on the organization if they are disclosed to unauthorized people?
    - Which assets will have a large adverse impact on the organization if they are modified without authorization?
    - Which assets will have a large adverse impact on the organization if they are lost or destroyed?
    - Which assets will have a large adverse impact on the organization if access to them is interrupted?
2. You should discuss the questions among yourselves. Remember that each of you brings a unique perspective to the discussion. When you come to a consensus and select the critical assets, start an *Asset Profile Workbook* for each critical asset. Note that there will be one workbook for each critical asset. Turn to the *Critical Asset Information* section of each *Asset Profile Workbook*.
3. In addition to selecting critical assets, you must also document your rationale for selecting those assets. To determine the rationale, you need to understand what aspect of the asset is important. This is especially true for the more complex assets (systems) where the assets have multiple characteristics. By understanding the important aspect of the asset and documenting the information, you will be better able to define security requirements and threats later in this workshop. Answering the following question might help you determine what is important about the asset:
    - Why is the asset critical to meeting the mission of your organization?

    When you come to a consensus, record the rationale for each critical asset in the *Critical Asset Information* section of its *Asset Profile Workbook*.
4. Note that there is also a place for a description of the asset. Consider the following questions as you discuss each critical asset:
    - Who controls the asset?
    - Who is responsible for the asset?
    - Who uses the asset?
    - How is the asset used?

    After discussing the questions, create a brief description for each critical asset. The description should include information elicited by the above questions.

A1.3	Identify Areas of Concern	
Worksheets Used in this Activity • *Areas of Concern* worksheet (W1.2) • *Asset workbook* for each critical asset	**Outputs of this Activity** • areas of concern for each critical asset	**Training** Use one asset

Basic Guidance

A threat is an indication of a potential undesirable event. It refers to a situation where a person could do something undesirable or where a natural occurrence could cause an undesirable outcome. An area of concern is a situation or scenario where someone is concerned about a threat to his or her important assets. Typically, areas of concern have a source and an outcome – a causal action that has an effect on the organization.

The following are the main sources that will be explored in this methodology:

- *deliberate actions by people* – This group includes people inside and outside your organization who might take deliberate action against your assets.
- *accidental actions by people* – This group includes people inside and outside your organization who might accidentally harm your assets.
- *system problems* – These are problems with your information technology (IT) systems. Examples include hardware defects, software defects, unavailability of related systems, viruses, malicious code, and other system-related problems.
- *other problems* – These are problems that are outside of your control. These can include natural disasters (e.g., floods and earthquakes) that can affect your organization's IT systems, unavailability of systems maintained by other organizations, and interdependency issues. Interdependency issues include problems with infrastructure services, such as power outages, broken water pipes, and telecommunication outages.

The resulting effect or outcome of scenarios typically fall into these categories:

- disclosure or viewing of sensitive information
- modification of important or sensitive information
- destruction or loss of important information, hardware, or software
- interruption of access to important information, software, applications, or services

A1.3 Identify Areas of Concern

Basic Guidance (cont.)

1. Refer to the *Areas of Concern* worksheet (W1.2). The worksheet contains prompts that focus on the sources and resulting outcomes of threat. The goal is to identify concerns about the important assets. The following are examples of areas of concern:
    - People are accidentally entering the wrong data into system XYZ. This results in incorrect records on that system.
    - Staff members often leave terminals/PCs unattended. This introduces the possibility of unauthorized access to the information on those systems.
2. For each selected asset, identify the groups of people (roles) known to the organization with some form of access to the systems who would be considered insiders (should have access granted) and outsiders (should be prevented from access). Hackers and groups outside of the organization should be included as outsiders. List these groups in the *Asset Profile Workbook* in the space labeled roles.
3. Identify areas of concern that identify a threat source which can result in an undesirable outcome of disclosure, modification, destruction or interruption of use to each asset. Consider potential differences in outcome if different roles are involved. List these in an *Asset Profile Workbook.*

A1.4	Identify Security Requirements for Important Assets	
Worksheets Used in this Activity	**Outputs of this Activity**	**Training**
• *Security Requirements* in Asset Profile Workbook	• Security requirements for assets	Use a single asset

Basic Guidance

The security requirements outline the qualities of an asset that are important to protect. This helps to form a basis for a protection strategy. The following are the security requirements to be examined:

- confidentiality – the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to see it
- integrity – the authenticity, accuracy, and completeness of an asset
- availability – when or how often an asset must be present or ready for use

Consider the *Security Requirements* page in the *Asset Profile Workbook*

- What are the important security requirements for each information asset?
- What is the relative ranking of the security requirements for each information asset? Which security requirement is the most important?

The first question focuses on describing the security requirements for each important asset. The second question asks the participants to select the requirement that is most important.

1. As you are thinking about the security requirements for the critical asset, consider the following questions:
   - Is this asset proprietary or sensitive? Does it contain personal information? Should it be inaccessible to anyone who is not authorized to see it? If the answer to any of these questions is yes, what is the specific confidentiality requirement?
   - Are authenticity, accuracy, and completeness important for this asset? If yes, what is the specific integrity requirement?
   - Is accessibility of the asset important? If yes, what is the specific availability requirement?
   - Are there any other security-related requirements that are important to this asset? What are they?

   When you come to a consensus, write the security requirements for the critical asset in the appropriate place in the *Security Requirements for Critical Asset* section of the workbook.
2. Next, you need to identify the most important security requirement for the critical asset. When you come to a consensus, note which security requirement is most important in the *Security Requirements for Critical Asset* section of the workbook.

A1.4 Identify Security Requirements for Important Assets

Additional Guidance

In general, when someone is trying to describe a security requirement for an asset, he or she needs to understand what aspect of the asset is important. This is especially true for the more complex assets (systems).

For *information assets*, the security requirements will focus on the confidentiality, integrity, and availability of the information. For example, the following is an example for information assets:

- The information must not be viewed by unauthorized personnel (confidentiality).
- The information can be modified only by authorized personnel (integrity).
- The information must be available whenever requested (availability).

Remember that *systems assets* generally represent groupings of information, software, and hardware assets. The specific aspect or quality of the system that is important will drive the security requirements. If the information stored, processed, and transmitted by the system is the most important aspect, then the following example describes the security requirements:

- The information on system XYZ must not be viewed by unauthorized personnel (confidentiality).
- The information on system XYZ can be modified only by authorized personnel (integrity).
- The information on system XYZ must be available whenever requested. Downtime for system XYZ can be only 15 minutes every 24 hours (availability).

If the service provided by the system is the most important aspect, then the following example describes the security requirements:

- The service provided by system XYZ must be complete and accurate (integrity).
- The service provided by system XYZ must be available whenever requested. Downtime for system XYZ can be only 15 minutes every 24 hours (availability).

Notice that no confidentiality requirement was listed. Confidentiality depends on what service is being provided. In many cases, the service is standard (Web), and confidentiality will not apply.

For *software assets*, you should focus on the software application or service when you identify security requirements. Do not focus on the information that is processed, transmitted, or stored by the application. If you find that this is how you are thinking about the software asset, then it is probably a systems or information asset. If the software is commercially or freely available, then confidentiality probably does not apply. If the software is proprietary to your organization, then there might be a confidentiality requirement. The following is an example for proprietary software assets. For commercially or freely available applications, ignore the confidentiality requirement.

A1.4 Identify Security Requirements for Important Assets

Additional Guidance (cont.)

- Application ABC must not be viewed by unauthorized personnel (confidentiality).
- Application ABC can be modified only by authorized personnel (integrity).
- Application ABC must be available during normal working hours (availability).

For *hardware assets*, you should focus on the physical hardware when you identify security requirements. Do not focus on the information that is processed, transmitted, or stored by the hardware. If you find that this is how you are thinking about the hardware asset, then it is probably a systems or information asset. Confidentiality does not apply to physical hardware. Modification of a hardware asset focuses on adding or removing hardware (for example, removing a disk drive or adding a modem). Availability focuses on whether the asset is physically available or accessible. The following is a guideline for hardware assets:

- The hardware can be modified only by authorized personnel (integrity).
- The hardware must be accessible during normal working hours (availability).

For *people assets*, you should focus only on the availability requirement. Remember, people assets are a special case. When people are identified, it is because of some special skill that they have or because of a service that they provide. Thus, availability of the service or asset is the primary requirement. The following is a guideline for people assets:

- The IT staff must provide ongoing system and network management services (availability).

Remember, when people are identified as assets, determine whether there are related assets. For example, identify a key system that they use or a type of information that they know. When you examine the security requirements for people assets, you might start to find out that the systems the people use are also important. However, be careful with extending this activity too far. If the people are part of another organization, you can stop after you identify them as an asset. Your main concern is the service that they provide to you. Their systems are beyond the scope of your information security risk assessment. If the people are part of your organization, then you can explore related assets.

A1.5 Capture Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

Worksheets Used in this Activity	Outputs of this Activity	Training
• *Current General Security Practices Survey* (W1.3) • *Current Educational Security Practices* (W1.4) • *Current IT Security Practices* (W1.5) • *Protection Strategy* worksheet (W1.6) • *Security Practices Summary* (W1.7)	• Survey results • Summary of current practices • Potential areas of organizational security concern	

Basic Guidance

The objective of a protection strategy is to provide a direction for future information security efforts rather than to find an immediate solution to every security vulnerability and concern. A protection strategy defines the strategies that an organization uses to enable, initiate, implement, and maintain its internal security.

1. Complete the three surveys: *Current General Security Practices Survey* (W1.3), *Current Educational Security Practices* (W1.4), and *Current IT Security Practices* (W1.5). Everyone should complete the first two surveys, and IT personnel should complete the third survey. The surveys are tied to security practices grouped according to categories constructed from a catalog of good practices. Consider which practices are used in their organization. Use the following options to define how your organization performs these practices:
    - Yes – The practice is used by the organization.
    - No – The practice is not used by the organization.
    - Unknown – The respondent does not know if the practice is used by the organization or not.
2. Review the *Protection Strategy* worksheet (W1.6). The following questions will be covered:
    - Which issues from the surveys would you like to discuss in more detail?
    - What important issues did the surveys not cover?
    - Are there specific policies, procedures, and practices unique to specific assets? What are they?
    - Do you think that your organization's protection strategy is effective? How do you know?

A1.5 Capture Knowledge of Current Protection Strategy Practices and Organizational Vulnerabilities

Basic Guidance (cont.)

The third question focuses on specific actions that members might take to protect certain assets. Sometimes an organization requires special policies, procedures, or practices for important information technology assets. The fourth question is broader and is intended to create a discussion of the general state of information security in the organization.

3. This discussion should uncover issues that are important to or unique to the organization.

   When discussing the first question, use the practice areas as well as questions of the survey as prompts for focusing attention. For example, "What is your impression of the organization's policies and procedures? Are they working?"

   The discussion will focus on what the organization is doing well (its current protection strategy) as well as what it is currently not doing well (its organizational vulnerabilities).

   The following are examples of protection strategy practices:

   + Technology enforces password changes and selection rules.
   + All employees have received security awareness training.

   The following are examples of organizational vulnerabilities:

   - While policies exist, they are not widely known.
   - People don't understand their security roles and responsibilities.

   In the above examples, a "+" indicates that the item is a protection strategy practice. A "–" indicates that the item is an organizational vulnerability.

4. Complete the *Security Practices Summary* (W1.7). Consider how well the survey covered existing security practices. Are any missing? Are any included that are irrelevant and should not be considered within the evaluation? Areas marked for "Needs Improvement" should be considered as vulnerabilities for the organization. Areas marked "Needs Research" should be evaluated with other resources and moved to one of the other status choices.

   Flag categories your organization is handling with using a "+" and categories not being handled well with a "-".

A1.6	**Identify Threats to Critical Assets**	
Worksheets Used in this Activity	**Outputs of this Activity**	**Training**
• *Asset Profile Workbook* for each critical asset (WK)	• Threats to critical assets	Focus on one asset

Basic Guidance

A threat is an indication of a potential undesirable event. It refers to a situation where a person could do something undesirable or where a natural occurrence could cause an undesirable outcome.

A threat profile defines the range of threats that can affect an asset. Threat profiles contain categories that are grouped according to source. The following list shows the threat categories that are considered:

- human actors using network access - These are network-based threats to your critical assets. These threats can be deliberate or accidental in nature.
- human actors using physical access - These are physical threats to your critical assets. These threats can be deliberate or accidental in nature.
- system problems – These are problems with your IT systems. Examples include hardware defects, software defects, unavailability of related systems, viruses, malicious code, and other system-related problems.
- other problems – These are problems that are outside of your control. These can include natural disasters (e.g., floods and earthquakes) that can affect your organization's IT systems, unavailability of systems maintained by other organizations, and interdependency issues. Interdependency issues include problems with infrastructure services, such as power outages, broken water pipes, and telecommunication outages.

In addition each threat comprises the following specific properties:

- asset – something of value to the organization
- actor – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset
- motive (optional) – defines whether the actor's intentions are deliberate or accidental
- access (optional) – how the asset will be accessed by the actor (network access, physical access)
- outcome – the immediate outcome (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset

Note that motive and access are optional. They apply only to human actors. Thus, motive and access are used for the following categories of threat: *human actors using network access* and *human actors using physical access*.

Threats can be visually represented in a tree structure. One tree exists for each threat category. Review the threat trees in the *Threat and Risk Profiles* section of the *Asset Profile Workbook*.

A1.6 Identify Threats to Critical Assets

Basic Guidance (cont.)

Note that there is one additional field in the trees – impact. Threat trees contain all fields with the exception of impact. A risk is the threat plus the resulting impact. The tree in this section of the workbook is actually a risk tree. However, during this activity, you will be addressing only the following properties: asset, access, actor, motive, and outcome. Thus, you will be addressing threats. Impact will be addressed during a later step.

1. Select a critical asset. Turn to the *Threat and Risk Profiles* section of that asset's *Asset Profile Workbook*.

   Review the areas of concern that affect the critical asset (from the *Areas of Concern* section of the *Asset Profile Workbook*). For each area of concern, decide which threat tree applies. Then decide which branches of the threat trees should be marked. Note that an area of concern could be mapped to multiple branches. Mark the appropriate branches of the threat tree in the workbook. Complete the applicable branches for all of the critical asset's areas of concern.

   Note the number of the area of concern on the branches that are marked by it to provide an audit trail back to the information that generated the tree.

2. Next you will need to address the unmarked branches. This activity is a gap analysis.

   Consider the following questions for the unmarked branches of a threat tree:

   - For which remaining branches is there a non-negligible possibility of a threat to the asset? (Mark these branches in the *Threat and Risk Profiles* section.)
   - For which remaining branches is there a negligible possibility or no possibility of a threat to the asset? (Do not mark these branches in the *Threat and Risk Profiles* section.)

   When missing branches should be marked, add the area of concern that is identified and mark the appropriate branches of the threat tree in the workbook. Remember to consider all branches for each threat tree.

3. After you have completed all of the threat trees, look at the outcomes across the threat profile. Compare the outcomes with the security requirements and address any gaps that exist.

   When comparing threat trees and security requirements, you must understand the relationships among the outcomes and the security requirements. The following table shows the relationships:

Security Requirement	Related Outcome
Confidentiality	Disclosure
Integrity	Modification
Availability	Loss, destruction, interruption

A1.6 Identify Threats to Critical Assets

Basic Guidance (cont.)

For example, if you have a security requirement for confidentiality, but no threats with disclosure as an outcome, you need to interpret the meaning of this situation. You should consider the following possibilities:

- Confidentiality is not a security requirement.
- You might have missed threats that result in disclosure of the critical asset.
- There is a negligible or no possibility of threats resulting in disclosure of the critical asset.
- The security requirement might be driven by law or regulation, not a threat.

Thus, you use the comparison of security requirements and threat trees to check for consistency and completeness.

Additional Guidance

When you map an area of concern to a threat tree, you need to think about the threat properties represented by the area of concern. For example consider the following areas of concern:

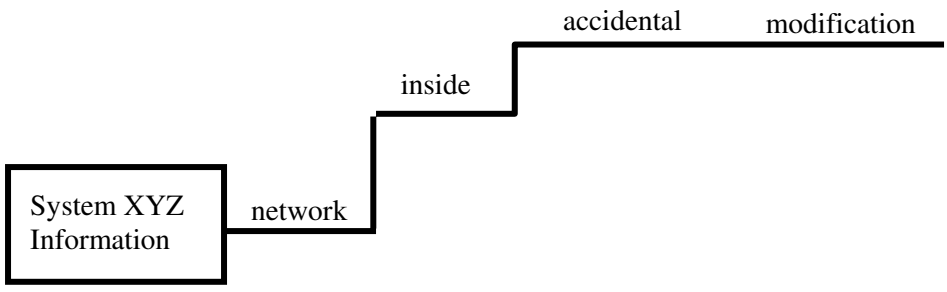
1. People are accidentally entering the wrong data into system XYZ. This results in incorrect records on that system.
2. Floods and other external events can lead to a denial of access to system XYZ.
3. Someone could use information from system XYZ for personal gain.

Note that in this example, the aspect of system XYZ that is important is the information on the system.

The following threat properties apply to the first area of concern:

- asset – system XYZ information
- access – network (The data are entered into a system.)
- actor – insiders (The concern implies staff with legitimate access.)
- motive – accidental
- outcome – modification (The data are incorrect; they have modified it.)

The first area of concern is mapped to the threat tree for *human actors using network access*. The following is the mapping for this threat:



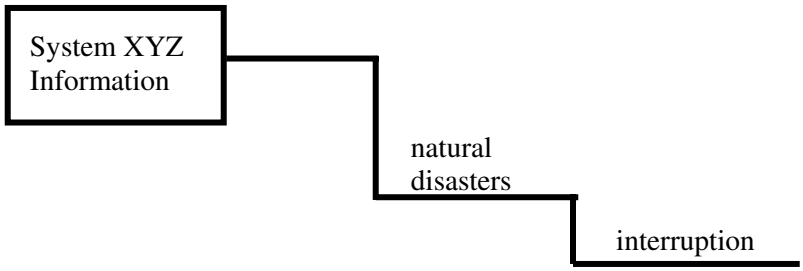
A1.6 Identify Threats to Critical Assets

Additional Guidance (cont.)

The following threat properties apply to the second area of concern:

- asset – system XYZ information
- actor – natural disasters
- outcome – interruption (of the access to the information)

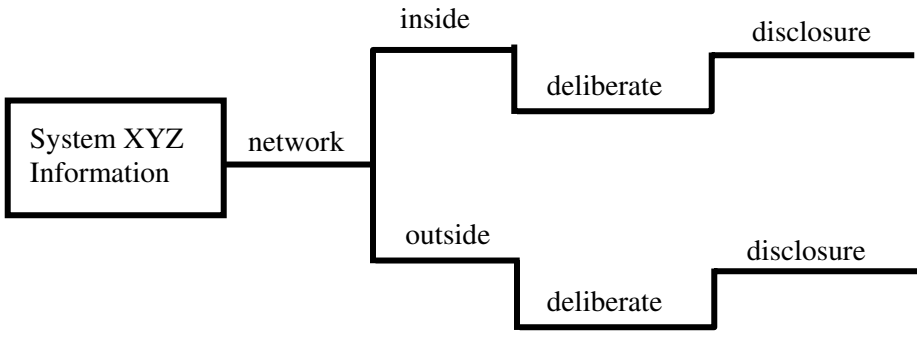
The second area of concern is mapped to the threat tree for *other problems*. The following is the mapping for this threat:



The following threat properties apply to the third area of concern:

- asset – system XYZ information
- access– network (The actor gets the information from the system.)
- actor – insiders and outsiders (The concern implies staff with legitimate access as well as outsiders.)
- motive – deliberate
- outcome – disclosure (The actor is viewing information that he or she shouldn't be viewing.)

The third area of concern is mapped to the threat tree for *human actors using network access*. The following is the mapping for this threat:



A1.6 Identify Threats to Critical Assets

Additional Guidance (cont.)

Note that the third area of concern actually represented two threats. An area of concern might map to multiple paths on the trees. You must use your judgment during this activity. Remember to keep your mind on the goal of this activity: to identify the range of threats to the critical asset.

Remember to add any notes that are relevant to the trees. This will be contextual information that elaborates on the information represented by the trees. For example, if a branch of the *human actors using network access* tree indicates an outside threat actor, you might want to add contextual notes. The threat might specifically refer to threats from hackers. If this is the case, then make sure that you add a note indicating that the outside threat refers to hackers. Other specific threats may tie to specific roles and these should be noted on the selected branches for clarity.

The *systems problems* and *other problems* threat trees contain very contextual threat actors. When you are mapping the areas of concern, you might find that the threat actor in the area of concern is not represented in the tree. An additional tree with no threat actors is provided in the *Asset Profile Workbook* for such cases. In addition, you can always add the additional threat actors directly to the *systems problems* and *other problems* threat trees in the workbook.

You should note that the category of asset will dictate which threat categories should be considered for a critical asset. The following information can be used as a guide to help you:

- For *information assets*, you need to determine whether the asset is represented electronically (on a systems asset), physically, or both. For electronic information, the following threat categories apply: human actors using network access, human actors using physical access, systems problems, and other problems. You should complete the threat trees for these categories.
- For information that is represented physically (on paper only), the following threat categories apply: human actors using physical access and other problems. You should complete the threat trees for these categories.
- *Systems assets* generally represent groupings of information, software, and hardware assets. The following threat categories apply to systems assets: human actors using network access, human actors using physical access, systems problems, and other problems. You should complete the threat trees for these categories.
- *Software assets* focus on software applications or services. The following threat categories apply to software assets: human actors using network access, human actors using physical access, systems problems, and other problems. You should complete the threat trees for these categories.
- *Hardware assets* focus on only the physical information technology hardware. The following threat categories apply to hardware assets: human actors using physical access and other problems. You should complete the threat trees for these categories.
- *People assets* focus on either a special skill that the people have or a service that they provide. The following threat category applies to people assets: other problems. You should complete the threat trees for this category only.

A1.7	**Identify Evaluation Criteria Areas**	
Worksheets Used in this Activity	**Outputs of this Activity**	**Training**
• *Identify Evaluation Criteria Areas* worksheet W1.8	• Evaluation criteria areas	--

Basic Guidance

The impact of a security problem can be felt within many areas of an organization. How are current programs and problems evaluated? What criteria are already in use within the organization to measure these areas?

- What criteria are used to define success or failure of projects?
- How are the criteria measured?
- Do the measurement criteria change if the considerations are administrative, teaching, or learning focused?
- Should the criteria be discussed with other groups in the organization? List.

The results of this discussion will be used in Phase 3 to establish evaluation criteria for weighing impacts should security risks be realized.

Risk Management K-12

Phase 2 Guidance: Technical View

Phase 2: Technology View

During Phase 2

	Activity	Description	Worksheets
A2.1	Identify Key Classes of Components	The analysis team establishes the system(s) of interest for each critical asset. The team then identifies the classes of components that are related to the system(s) of interest.	*Asset Profile Workbook*
A2.2	Identify Infrastructure Components to Examine	The analysis team selects specific components to evaluate. The system(s) of interest is automatically selected for evaluation. The team selects one or more infrastructure components from each key class to evaluate. In addition, the team also selects an approach and specific tools for evaluating vulnerabilities.	*Asset Profile Workbook*
A2.3	Run Vulnerability Evaluation Tools on Selected Infrastructure Components	The IT staff or external experts conduct the vulnerability evaluation. They are responsible for running the vulnerability evaluation tools and creating a vulnerability summary for each critical asset prior to the workshop.	---
A2.4	Review Technology Vulnerabilities and Summarize Results	The IT staff members or external experts who ran the vulnerability tool(s) present a vulnerability summary for each critical asset and interprets it for the analysis team. Each vulnerability summary is reviewed and is refined if appropriate.	*Asset Profile Workbook*

A2.1 Plan Vulnerability Assessment

Worksheets Used in this Activity	Outputs of this Activity	Training
• *Asset Profile Workbook* for each critical asset	• key classes of components	Use one asset

Basic Guidance

1. Select a critical asset. You will examine only the threat tree for *human actors using network access* during this activity. This threat tree defines the range of scenarios that threaten the critical asset due to deliberate exploitation of technology vulnerabilities or accidental actions by people.
2. Turn to the *Threat and Risk Profiles* section of the *Asset Profile Workbook* for the critical asset. Review the scenarios represented by the threat tree for *human actors using network access*. If the tree for *human actors using network access* has no threats marked, then you will not need to complete this activity for the critical asset.
3. If threats for *human actors using network access* exist for the critical asset, then turn to the *Asset Profile Workbook* section of *Identify System of Interest*.
4. First, you will establish the system of interest for the critical asset (where does it "live" in the technology infrastructure). Review the threat tree for "human actors using network access" in this workbook and determine the system(s) of interest for the critical asset. Use the following questions to guide your selection of the system(s) of interest:
    - Which system(s) is most closely linked to the critical asset? In which system(s) is the critical asset stored and processed?
    - Where outside of the system of interest do critical information assets move? Backup system? Off-site storage? Other?
    - Based on the critical asset, which system(s) would be the target of a threat actor acting deliberately?

    Record it in the appropriate place in the *Asset Profile Workbook*.

    The components that you will evaluate in A2.3 for technology vulnerabilities will be part of or related to the system of interest. You should also note that you might have multiple systems of interest for a critical asset. This might happen if
    - a group of interrelated systems collectively performs a unique function or meets a unique objective
    - a group of interrelated systems has common or overlapping functions
    - a critical asset is closely linked to multiple systems

A2.1 Plan Vulnerability Assessment

Basic Guidance (cont.)

5. You will now examine key classes of components that are a part of or are related to the system of interest. These are classes of components used by legitimate users when they access the critical asset. Threat actors also use the key classes of components when they deliberately attempt to access the critical asset. Consider the following questions from the *Key Classes of Components* section of the *Asset Profile Workbook*:

    - Which types of components are part of the system of interest? Consider servers, networking components, security components, desktop workstations, home machines, laptops, storage devices, wireless components, and others.
    - Which types of components are related to the system of interest? From which types of hosts can the system of interest be legitimately accessed? Desktop machines? Home machines? Laptops? Cellular phones? Handheld devices? Others?
    - How could threat actors access the system of interest? Via the Internet? Via the internal network? Shared external networks? Wireless devices? Others?
    - Which types of components could a threat actor use to access the system of interest? Which could serve as intermediate access points? Consider physical and network access to servers, networking components, security components, desktop workstations, home machines, laptops, storage devices, wireless components, and others.
    - What other systems could a threat actor use to access the system of interest?
    - Based on your answers to the above questions, which classes of components could be part of the threat scenarios?

    When you come to a consensus on which classes of components could be part of the threat scenarios, the scribe should mark an "X" in the box by each of the classes. In addition, document your rationale for selecting this class of components.

    If there are classes of components that are important to analyzing potential threats to the system of interest but not provided in the list, be sure and add them.

A2.1 Plan Vulnerability Assessment

Additional Guidance

The system of interest is a system that gives a threat actor access to a critical asset. It is also the system that gives legitimate users access to a critical asset. The following are general guidelines to help you identify the system of interest:

- For *systems assets*, the system of interest is the asset.
- For *information assets*, the system of interest is the system that is most closely linked to the information. It can be where the critical information asset is stored and processed. It can also be where the critical information asset moves outside the network (backup systems, off-site storage, other storage devices).
- For *software assets*, the system of interest is the system that is most closely linked to the software application or service. It can be the system from which the critical software asset is served or where it is stored.

It is possible to have multiple systems of interest for information and software assets because they might be closely linked to multiple systems.

Distributed assets, such as the network, might comprise multiple systems of interest. For distributed critical assets, you have a couple of options when identifying the system(s) of interest. You might realize that the critical asset is defined too broadly. You could then define the critical asset more narrowly. Alternatively, you can accept how the critical asset is defined and identify multiple systems of interest for that critical asset.

Access paths focus on how information or services can be accessed via your organization's network. They are important when you are identifying key classes of components. When you identify key classes of components, you will most likely refer to information about your computing infrastructure. The following list highlights three potential sources of information about your computing infrastructure:

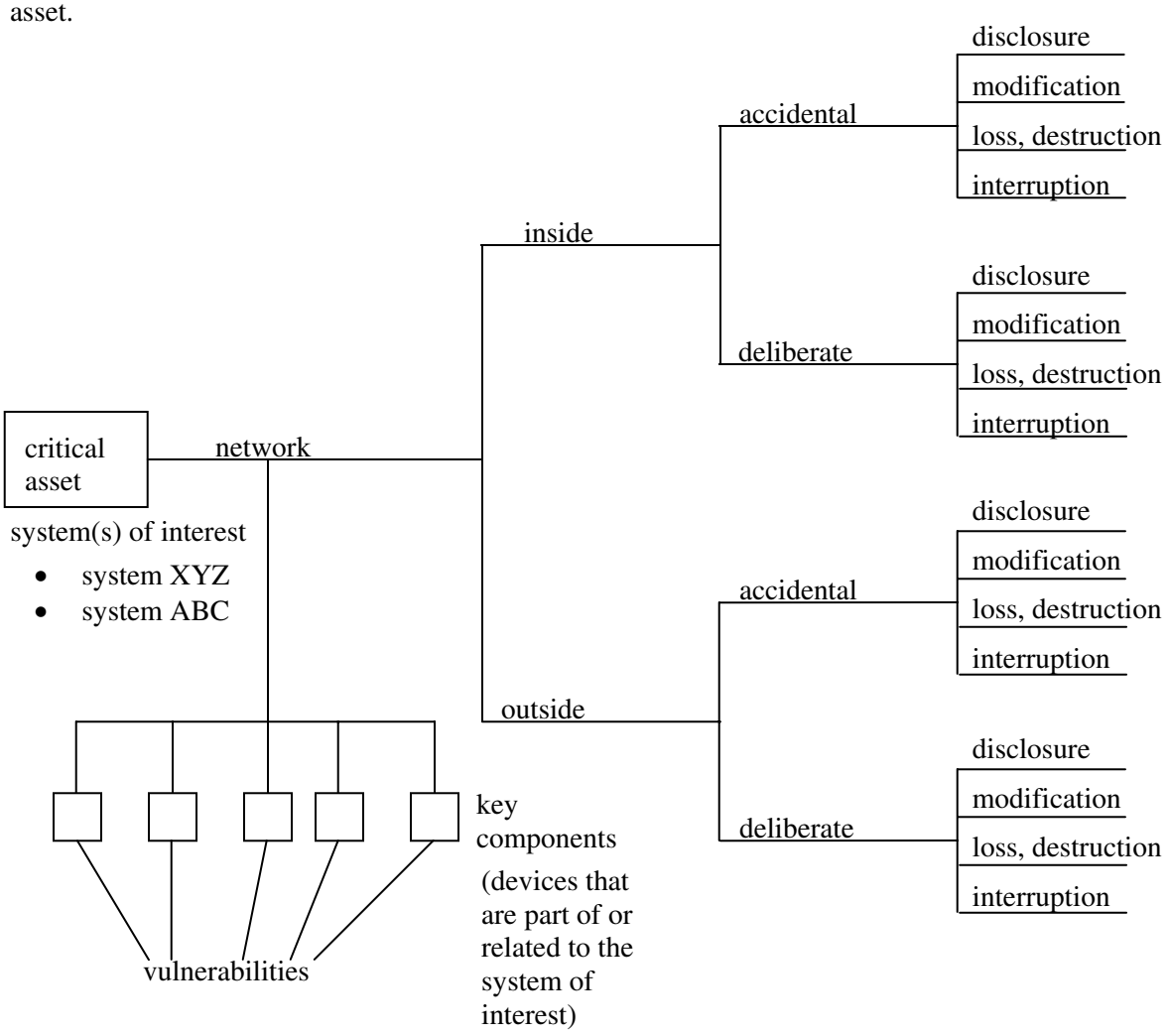
- Network mapping tools – software used to search a network, identifying the physical connectivity of systems and networking components. The software also displays detailed information about the interconnectivity of networks and devices (routers, switches, bridges, hosts).
- Network topology diagrams – electronic or paper documents used to display the logical or physical mapping of a network. These documents identify the connectivity of systems and networking components. They usually contain less detail than that provided by network mapping tools.
- Computer prioritization listings – a listing of the computer inventory owned by an organization. This listing typically depicts a prioritized ordering of systems or networking components based on their importance to the organization (e.g., mission critical systems, high/medium/low priority systems, administrative systems, support systems, etc).

Any of the above sources of information can be used. You need to decide how much and what type of information you need to select the key classes of components.

A2.1 Plan Vulnerability Assessment

Additional Guidance (cont.)

The diagram below shows the threat tree for *human actors using network access*. Notice that the key components and vulnerabilities are shown in the diagram. You can see that vulnerabilities in these key components create a means by which threat actors can exploit the vulnerabilities and access the critical asset.



A2.2 Identify Infrastructure Components to Examine

Worksheets Used in this Activity	Outputs of this Activity	Training
• *Asset Profile Workbook* for each critical asset	• infrastructure components to examine • selected approach for evaluating each infrastructure component	Use one critical asset

Basic Guidance

During the previous activity, you identified the system(s) of interest for critical assets as well as key classes of components that are part of or related to the system(s) of interest. In this activity, you will select one or more infrastructure components from each class to evaluate for technology vulnerabilities.

1. Select a critical asset. Turn to the *Selected Components for Evaluation* section of that asset's *Asset Profile Workbook*. During this activity, you will be answering the following questions for each class of components:
    - Which specific component(s) in this class will we evaluate for vulnerabilities?
    - What is our rationale for selecting this specific component(s)?
    - What approach will we use to evaluate each selected component?
2. Review your organization's network topology diagram in relation to each key class of component that you identified during the previous activity. You must determine how many infrastructure components to evaluate from each class. You need to evaluate enough components from each class to get a sufficient understanding of the vulnerability status of a "typical" component from the class (see *Additional Guidance* for more information). As you select specific components to evaluate, consider the following questions:
    - Is the infrastructure component typical of its class?
    - How accessible is the infrastructure component? Is it "owned" by another organization? Is it a home machine?
    - How critical is the infrastructure component to business operations? Will you be interrupting business operations when you evaluate the component?
    - Will special permission or scheduling be required to evaluate the component?

    When you select a specific component, you also need to record the Internet Protocol (IP) address and the host/domain name system (DNS) name (fully qualified domain name) for the component. See the *Additional Guidance* for this activity for more information on IP addresses and host/DNS names.

    Remember to select one or more component in each key class. When you select an approach for evaluating an infrastructure component, you need to consider who will be performing the evaluation as well as which tool(s) will be used.

A2.2 Identify Infrastructure Components to Examine

Basic Guidance (cont.)

Once you have selected a component add the following information to the table in the *Selected Components for Evaluation* section of the workbook for each key class of component:

- selected components, including IP addresses and host/DNS names (fully qualified domain names)
- rationale
- an approach for evaluating each infrastructure component, including who will perform the evaluation and the selected tool(s)

Note that you might identify a number of action items during this activity. Before you run any tools on your organization's networks, you will need to obtain appropriate management approval. In addition, you might decide that you need to research available vulnerability evaluation tools in order to make good decisions about selecting tools. You might need to acquire the selected tools or need to be trained in their use. Make sure that you record any action items and assign responsibility for completing them.

3. Keep in mind that some components will be important to more than one critical asset. As you select components to evaluate, look for any overlaps and redundancy across critical assets.

Additional Guidance

In selecting specific components to include in a vulnerability evaluation, you need to balance the comprehensiveness of the evaluation with the effort required to evaluate the components. For example, if you have selected desktop workstations as a key class of components, you need to select one or more workstations to include in your vulnerability evaluation. If you have a thousand desktop workstations in your organization, you need to decide how many you should include in the technology evaluation. Your goal should be to get a feel for the vulnerability status of a typical workstation. You will probably decide to look at more that one workstation. However, you probably need to evaluate only a handful of workstations to get a sufficient understanding of the vulnerability status.

In general, you want to make sure that you have enough information to understand the vulnerability status of the key class, but you don't want to select so many components that you have trouble sorting through all of the data. You need to determine when you have enough information to move forward in the process. You want to make sure that you don't collect too little information about a key class and that you don't collect too much information about the class. Use your best judgment.

When you select specific infrastructure components to evaluate, you also need to record their Internet Protocol (IP) addresses and host/DNS names. In larger organizations, IP addresses can change on a daily basis for many components, although this is not likely for servers, routers, and firewalls. Recording the fully qualified domain name of the component helps to identify it more reliably than the IP address alone because of services like DHCP (dynamic host configuration protocol), where the IP address changes each time a machine boots.

A2.2 Identify Infrastructure Components to Examine

Additional Guidance (cont.)

As you move from one critical asset to the next, you will find that many of the same key classes apply to many of the critical assets. The components that you select for a key class related to one critical asset will probably be sufficient for the same key class for another critical asset. Again, you must use your best judgment.

It is important for you to keep in mind that understanding risk is the ultimate goal of this evaluation. You only need enough vulnerability information to understand how vulnerable your computing infrastructure currently is. Do not attempt to look at every component – the volume of information will become overwhelming. Examining every component of your computing infrastructure over a defined period of time is part of a vulnerability management process. Vulnerability management might already be a practice in your organization, or establishing a vulnerability management process might be a part of the protection strategy or risk mitigation plans that you will develop in Phase 3.

When you select an approach for evaluating an infrastructure component, you are determining how the evaluation will be performed. You are deciding whether your information technology staff will perform the evaluation or whether you intend to outsource the evaluation to external experts. You are also deciding which tool(s) will be used during the evaluation.

If you decide that your organization will perform the evaluation, you need to identify the software tool(s) that you will use. You also need to identify the people who will perform the evaluation and interpret the results. Make sure that you have permission to run any tools on your site's infrastructure. Also, make sure that you set a specific schedule for running the tools and that you let all stakeholders know what you intend to do and when you intend to do it.

If you decide to outsource, you should think about how you will communicate your needs and requirements to the external experts and how you intend to verify whether they have sufficiently addressed those needs and requirements. Also, make sure that the experts set a specific schedule for running any tools on your networks and that they let all stakeholders know what they intend to do and when they intend to do it.

Some organizations use contractors or managed service providers to maintain their systems and networks. If contractors or personnel from managed service providers are going to participate in the vulnerability evaluation, you need to decide how to include them. They can be included on the analysis team, or you could treat them as external experts. It depends on the nature of the working relationship that your organization has with them.

You must also decide which tool(s) you will use. Tools include software, checklists, and scripts. You need to decide whether you intend to automate the process of evaluating technology vulnerabilities (by using software), or if you intend to use checklists or scripts. Once you have made this decision, you need to select the specific tools, checklists, or scripts.

Software tools assess a system or systems, identifying known weaknesses (exploits) and misconfigurations. They also provide information about the potential for success if an intruder were to attempt an intrusion. These types of tools are often used by intruders when they attack an organization's systems and networks. The intruder will commonly scan systems remotely from the Internet to find vulnerabilities. These scans can provide the intruder with the means to access (read, modify, or destroy) and interrupt (deny availability of) your systems and networks.

A2.2 Identify Infrastructure Components to Examine

Additional Guidance (cont.)

The following list highlights types of vulnerability identification tools that you should consider:

- Operating system scanners – target specific operating systems such as Windows NT/2000, Sun Solaris, Red Hat Linux, or Apple Mac OS.
- Network infrastructure scanners – focus on the components of the network infrastructure, such as routers and intelligent switches, DNS (domain name system) servers, firewall systems, and intrusion detection systems.
- Specialty, targeted, or hybrid scanners – target a range of services, applications, and operating system functions. For example, they may deal with Web servers (CGI, JAVA), database applications, registry information (e.g., Windows NT/2000), and weak password storage and authentication services.
- Checklists – provide the same functionality as automated tools. However, unlike automated tools, checklists are manual, not automated. They also require a consistent review of the items being checked and must be routinely updated.
- Scripts – provide the same functionality as automated tools, but they usually have a singular function. The more items you test, the more scripts you'll need. Again, as with checklists, scripts require a consistent review of the items being checked and must be routinely updated.

The reports generated by software tools provide a wide range of content and format. You need to first determine what information you require, and then you need to match your requirements to the report(s) provided by the tool(s).

You should also consider how much information each tool provides and whether it provides any means to filter or interpret the information. The reports that are generated by software tools can be quite long (300+ pages), especially when a large number of systems are scanned.

Vulnerability tools do have limitations. They will not indicate when system administration is being improperly or incorrectly performed. For example, a tool will not be able to determine whether users are being given access to more information or services than they need. The information technology staff needs to follow good practices for defining required security levels, setting up and managing accounts, and configuring infrastructure components.

Vulnerability tools check only for known vulnerabilities; the tools will not identify unknown vulnerabilities or new vulnerabilities. Thus, you need to ensure that you keep your vulnerability tools current with the latest vulnerability information that is provided by vendors and by other sources of vulnerability information.

Finally, vulnerability tools will not indicate whether staff members are following good practices (e.g., if staff members have shared passwords or ignored physical security procedures) or whether implemented security rules are in-line with your business objectives. This is why the surveys and protection strategy discussion from Phase 1 are so important; they evaluate aspects of security that tools can't examine.

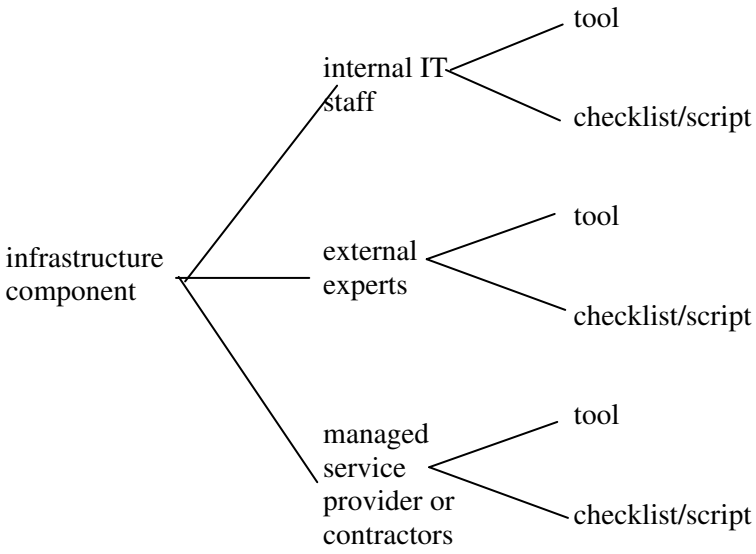
A2.2 Identify Infrastructure Components to Examine

Additional Guidance (cont.)

Some automated tools have the potential for causing interruptions in service or other problems when they are run. Much of this depends upon your particular systems and the way they are configured. The analysis team and any supplemental members need to discuss the possibilities for what could occur and determine who would be affected should anything happen.

Cost estimates may also be required, particularly if tools need to be purchased or upgraded, or if someone needs to be trained to run the tools. Other costs that you must consider include personnel time to coordinate and run the tools as well as time lost by staff members who might not be able to perform their duties efficiently when testing occurs.

The following diagram illustrates the choices that you must consider when creating an approach for evaluating an infrastructure component for technology vulnerabilities (all choices require consideration for incorporating the latest catalog of vulnerabilities for currency of information):



A2.3 Run Vulnerability Evaluation Tools on Selected Infrastructure Components

Worksheets Used in this Activity	Outputs of this Activity	Activity Time
---	• technology vulnerabilities • proposed technology vulnerability summary	---

Basic Guidance

During this activity, the IT staff or external experts conduct the vulnerability evaluation. They are responsible for running the vulnerability evaluation tools and creating detailed vulnerability reports prior to the workshop.

1. Before using vulnerability evaluation tools, designated personnel (IT staff members or external experts) must verify that
   - the correct tool(s) is being used
   - the latest version of the tool(s) is being used and the most up-to-date catalog of vulnerabilities is incorporated
   - all necessary approvals have been obtained and that all affected personnel have been notified
   - any other action items from A2.1 & A2.2 have been completed
2. Designated personnel (IT staff members or external experts) run vulnerability evaluation tools on the selected infrastructure components identified during A2.2. Members of the analysis team can be present to observe the evaluation, or they can directly participate in the evaluation, if appropriate. If the designated personnel are unable to examine an infrastructure component for technology vulnerabilities, then they need to document the reason. The situation must be discussed with the analysis team during the A2.4 activity.
3. Designated personnel (IT staff members or external experts) review the detailed vulnerability information generated by the tool(s), interpret the results, and create a preliminary summary of the technology vulnerabilities for each key component.

   The vulnerability summary for each component will contain the following information for each component that was evaluated:
   - the number of vulnerabilities to fix immediately (high-severity vulnerabilities)
   - the number of vulnerabilities to fix soon (medium-severity vulnerabilities)
   - the number of vulnerabilities to fix later (low-severity vulnerabilities)

A2.3 Run Vulnerability Evaluation Tools on Selected Infrastructure Components

Additional Guidance

Software vulnerability evaluation tools should collect the following types of information for each selected component:

- vulnerability name
- description of the vulnerability
- severity level of the vulnerability
- actions required to plug the vulnerability

Vulnerability evaluation tools check for known technology vulnerabilities. No matter which type of tool (software, checklists, scripts) is selected to evaluate infrastructure components, it must be able to check components for known weaknesses (exploits) and inappropriate configurations. Vulnerability evaluation tools check for known weaknesses and bad configurations by relying upon a catalog of vulnerabilities. A catalog of vulnerabilities is a collection of known technological weaknesses, based on platform and application.

One catalog of vulnerabilities commonly used is the Common Vulnerabilities and Exposures (CVE). CVE is a list or dictionary that provides common names for publicly known vulnerabilities. CVE is a community effort led by MITRE Corporation that can be accessed at http://www.cve.mitre.org. CVE enables open and shared information without any distribution restrictions.

You should always make sure that you have proper permission and management approval prior to running vulnerability evaluation tools on your networks. The IT department should have procedures for obtaining approval to use the vulnerability evaluation tools.

The need for a preliminary summary is based on the assumption that the vulnerability evaluation is not conducted by all of the analysis team members. Software vulnerability evaluation tools produce very detailed reports that are not easily understood by personnel who do not have information technology *and* security backgrounds. Checklists and scripts also require considerable information technology and security expertise to use. Thus, the assumption that business staff members observe, but do not necessarily actively participate, in the vulnerability evaluation will often be true.

Remember that some of the analysis team members must be business staff members who probably do not configure and manage systems on a day-to-day basis. In many cases, the skills of the core analysis team members will be augmented by including additional IT staff members or external experts to conduct the vulnerability evaluation. If the IT staff members or external experts conduct the evaluation, then a preliminary vulnerability summary is necessary to communicate vulnerability information to the core analysis team members. The summary should be presented to the analysis team during the workshop.

A2.4	Review Technology Vulnerabilities and Summarize Results	
Worksheets Used in this Activity	**Outputs of this Activity**	**Training**
• *Asset Profile Workbook* for each critical asset	• technology vulnerability summary	--

Basic Guidance

1. Select a critical asset for which a vulnerability evaluation was conducted. Turn to the *Vulnerability Summary* section of that asset's *Asset Profile Workbook* (WK).

   For each evaluated component, you will first review the summary of the vulnerability evaluation that was created by IT staff or external experts who conducted the evaluation. The summary will contain the following information for each component that was evaluated:

   - the number of vulnerabilities to fix immediately (high-severity vulnerabilities)
   - the number of vulnerabilities to fix soon (medium-severity vulnerabilities)
   - the number of vulnerabilities to fix later (low-severity vulnerabilities)

2. For each selected component, review and discuss the summary of the technology vulnerabilities that were identified. The IT staff or external experts who conducted the evaluation will lead the discussion of the summary and will interpret the results for you.

   Remember that the analysis team comprises information technology staff members (who have an understanding of the implication of technology vulnerabilities) as well as business staff members (who probably do not have an understanding of the implication of technology vulnerabilities). The person(s) presenting the vulnerability evaluation summary must make sure that all members of the analysis team understand

   - the types of vulnerabilities found and how these put the asset at risk
   - when they need to be addressed to avoid a possible exploit
   - the potential effect on the critical assets
   - how the technology vulnerabilities could be addressed (applying a patch, hardening a component, etc.) and other potential areas the steps taken to address the vulnerability could impact.

   Everyone on the analysis team needs to understand the summary.

A2.4 Review Technology Vulnerabilities and Summarize Results

Basic Guidance (cont.)

Once the summary is reviewed and refined, the scribe will record the summary in the appropriate place in the *Vulnerability Summary* section of the asset's *Asset Profile Workbook.*

You should note that only the summaries are recorded in the *Asset Profile Workbook*. The detailed reports generated by the tools should also be kept and used after the evaluation when the vulnerabilities are being addressed.

In addition, any specific actions or recommendations for addressing the technology vulnerabilities should be recorded in the *Vulnerability Summary* section of the asset's *Asset Profile Workbook*. This information will be useful during Phase 3, when you will create risk mitigation plans and an action list.

If you need to address any technology vulnerabilities immediately, make sure that you assign an action item and designate responsibility for it.

3. After you have reviewed and discussed the vulnerability summary, you should perform a gap analysis of the threat profile that you created during Phase 1. Turn to the *Threat and Risk Profiles* section of the critical asset's *Asset Profile Workbook.* You must reexamine the unmarked branches of the threat tree for *human actors using network access*. Consider the following question when you are reviewing the unmarked branches of a threat tree:

    - Do the technology vulnerabilities associated with the critical asset's key infrastructure components indicate that there is a non-negligible possibility of a threat to the asset? (Mark these branches in the *Threat and Risk Profiles* section.)

    Be sure and describe the *Area of Concern* that has generated this additional threat and note the link to the vulnerability assessment.

4. Once you have completed this activity for the critical asset, move on to the next critical asset. Continue with this activity until you have completed a vulnerability summary for each critical asset and have recorded the summary in the appropriate *Asset Profile Workbook.*

A2.4 Review Technology Vulnerabilities and Summarize Results

Additional Guidance

Technology vulnerabilities are weaknesses in systems that can directly lead to unauthorized action. In many cases, poor organizational practices can lead to the existence of technology vulnerabilities.

Technology vulnerabilities are present in and apply to network services, architecture, operating systems, and applications. Technology vulnerabilities are often grouped into three categories:

1. *design vulnerabilities* – a vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability
2. *implementation vulnerabilities* – a vulnerability resulting from an error made in the software or hardware implementation of a satisfactory design
3. *configuration vulnerabilities* – a vulnerability resulting from an error in the configuration and administration of a system or component

In addition, technology vulnerabilities can be used to refine the picture of current security practices used by staff as well as organizational vulnerabilities that are present in the organization. A technology vulnerability can result from many sources: a user's lack of awareness regarding information security policy and practice, deliberate avoidance or circumventing of existing policy and practice, insufficient training and readiness to address information security vulnerabilities, misplaced or inappropriate trust, etc.

Technology vulnerabilities can directly refine the current practice survey results with respect to Information Technology Security (see Security Practices Summary W1.7). You should look for patterns that can help you better understand the security issues. For example, staff members may indicate that they perform a practice, but the pattern of technology vulnerabilities might show evidence to the contrary. Review patterns of technology vulnerabilities that affect a critical asset as well as patterns of technology vulnerabilities across critical assets.

As you draw conclusions based on the patterns of technology vulnerabilities, remember to record any specific actions or recommendations in the *Vulnerability Summary* section of the appropriate *Asset Profile Workbook(s)*.

Technology vulnerabilities also define the access paths that human threat actors can use to access a critical asset. Recall that a system of interest is the system that is most closely linked to a critical asset Each system of interest has several key infrastructure components that are part of or related to the system. Key infrastructure components are types of devices that are important in processing, storing, or transmitting the critical information associated with the system of interest. When you identify a technology vulnerability on a key infrastructure component, you have identified a weakness that can directly lead to unauthorized action by a threat actor.

A2.4 Review Technology Vulnerabilities and Summarize Results

Additional Guidance (cont.)

A high-severity vulnerability, by definition, is a major weakness that needs to be addressed immediately. If a threat actor exploits a high-severity vulnerability, it will directly lead to a violation of the security requirements for the critical asset. One of the outputs of this process might be an action item to address all high-severity vulnerabilities. A low-severity vulnerability, by definition, is a weakness that can be addressed at a later time. This does not mean that you can forget about it. A threat actor can exploit a sequence of low-severity vulnerabilities and produce a similar effect to that resulting from exploiting a high-severity vulnerability. Normally, it takes a sophisticated actor to do this.

The outputs of the Risk Methodology include a protection strategy and risk mitigation plans. When you develop either output, you might consider what to do about managing vulnerabilities. A vulnerability management process includes

- examining every component of your computing infrastructure over a defined period of time
- addressing the vulnerabilities that you identify

By implementing a vulnerability management process, you can more effectively address vulnerabilities of all severity levels.

Risk Methodology K-12

Phase 3 Guidance: Strategy and Plan Development

During the Workshop

	Activity	Description	Worksheets
A3.1	Identify the Impact of Threats to Critical Assets	The analysis team defines impact descriptions for threat outcomes (disclosure, modification, loss, destruction, interruption). The impact description is a narrative statement that describes how a threat ultimately affects the organization's mission. The combination of a threat and the resulting impact to the organization defines the risk to the organization.	*Asset Profile Workbook*
A3.2	Create Risk Evaluation Criteria	The analysis team creates evaluation criteria that will be used to evaluate the risks to the organization. Evaluation criteria define what constitutes a high, medium, and low impact.	*Asset Profile Workbook*
A3.3	Evaluate the Impact of Threats to Critical Assets	The analysis team reviews each risk and assigns it an impact measure (high, medium, or low).	*Asset Profile Workbook*
A3.4	Create Mitigation Plans	Create risk mitigation plans for each critical asset. A mitigation plan defines the activities required to mitigate the risk/threats to the critical assets.	*Asset Profile Workbook* *Security Practices Summary* worksheet (1.7)
A3.5	Create Action Plans	Create action plans for near term activities that are needed to address security areas but do not require specialized training, policy changes, or other longer-term steps.	*Asset Profile Workbook* *Security Practices Summary* worksheet (1.7)
A3.6	Organization Protection Strategy	Create a protection strategy for the organization. This strategy defines how the organization will enable, initiate, implement, and maintain its internal security	*Security Practices Summary* worksheet (1.7) *Asset Profile Workbooks*

A3.1 Identify the Impact of Threats to Critical Assets

Worksheets Used in this Activity	Outputs of this Activity	Training
• *Asset Profile Workbook* for each critical asset • *Identify Evaluation Criteria* worksheet 1.8	• Impact of threats to critical assets	Use one asset

Basic Guidance

During this activity, you will define impact descriptions for threat outcomes. You can use any materials that will help you in your decision making.

Risk is the possibility of suffering harm or loss. It comprises a threat to a critical asset and the resulting impact to the organization. Thus, when you add the impact to the organization to a threat, you create a risk. In this activity, you will be describing the impacts for the threat profiles created in Phase I.

1. Select a critical asset. Turn to the *Threat and Risk Profiles* section of the *Asset Profile Workbook*. Review the threat profile for the critical asset. Recall that the threat profile defines the range of threat scenarios to the critical asset. Make sure that you note which outcomes have been marked in the profile. Remember to look at all of the threat trees in the profile. You should also review the areas of concern recorded in the *Areas of Concern* section of the workbook.
2. Turn to the *Impact Descriptions* section of the asset's *Asset Profile Workbook*. The section contains a table for each of four threat outcomes (disclosure, modification, loss/destruction, interruption). During this activity, you will fill out each table that is appropriate for the critical asset.

   If disclosure, modification, loss/destruction, or interruption is the outcome of one or more threats in the profile, then complete its respective table in the workbook.

   For any threat outcome that is not marked at least once in the threat profile for the critical asset, do not fill out the table for that outcome.

   For each table that you fill out, consider the impact areas listed in the table and then create a narrative description for each impact. Note that you can have multiple impacts for each threat outcome.

   Expand the list of impact areas to include all important evaluation criteria identified in Phase I.

A3.2	Create Risk Evaluation Criteria	
Worksheets Used in this Activity • *Evaluation Criteria* worksheet 3.2 • *Identify Evaluation Criteria* worksheet 1.8	**Outputs of this Activity** • risk evaluation criteria	**Training** Select a subset of criteria

Basic Guidance

During this activity, you will be creating evaluation criteria to apply to impacts across all assets. Evaluation criteria are benchmarks or measures against which you will evaluate the impacts that you described during the previous activity. Evaluation criteria are created for a broad range of impact types, or categories. The categories of impact for which you will be creating evaluation criteria are

- regulatory compliance
- classroom plans and curriculum effectiveness
- life/health/safety of students, teachers, and staff
- student performance on standardized tests and evaluations
- family and community support
- school and district administration support
- teacher preparation
- other

These categories should be adjusted based on information from *Identify Evaluation Criteria* worksheet 1.8

During this activity, you will define what constitutes a high, medium, and low impact for each of the impact categories. Make sure that you review the impact information that you documented during the previous activity (in the *Impact Descriptions* section of the *Asset Profile Workbook*). This can be useful for defining the evaluation criteria.

1. Select a critical asset. Turn to the *Evaluation Criteria* worksheet 3.2.
2. For each impact area in the table, consider what specific measures you will use for high, medium, and low risks. If you need an example of evaluation criteria, review the *Example Results.*
3. If an impact area is not applicable to your organization, then note it in the table. Do not define measures that do not apply to your organization. For any impact areas that are unique to your organization, add those measures in the "other" category.

A3.2 Create Risk Evaluation Criteria

Additional Guidance

Risks are evaluated to provide additional information to assist decision makers. An organization cannot mitigate every risk because of funding, staff, and schedule constraints. Thus, it is necessary to determine relative priorities. In many risk management processes, both impact and probability are evaluated as a means of deciding which risks to deal with first, if at all.

Consider a simple example. A manager may choose to deal with only high-impact, high-probability risks; to keep an eye on medium-impact, medium-probability risks; and to ignore low-impact, low-probability risks. Thus, the manager is using impact and probability to guide his or her choices.

In this methodology, only the impact of a risk is evaluated. For information security risks, probability is a more complex and imprecise variable than is normally found in other risk management domains. It is unreasonable, for example, to attempt to calculate the probability of an unknown teenager from an unknown country with unknown motivations performing a port scan on your server and finding a way in. Even if the probability could be calculated, it would change minute by minute based on numerous factors.

The qualitative measures of high, medium, and low provide the simplest means of assigning values to risk impacts. These measures provide enough of a benchmark to compare impacts across all critical assets.

Evaluation criteria are highly contextual. For example, while $1,000,000 may be a high impact to one organization, it could be only a medium or low impact to another. Also, some organizations will have risks that result in a loss of life, but this is not true for all organizations. The contextual nature of evaluation criteria is the reason why every organization must define its own criteria.

A3.3 Evaluate the Impact of Threats to Critical Assets

Worksheets Used in this Activity	Outputs of this Activity	Training
• *Asset Profile Workbook* for each critical asset	• impact values	Use one critical asset

Basic Guidance

During this activity, you will be working as a team to evaluate risks. You can use any materials that will help you in your decision making. Some suggestions are

- *Impact Descriptions* section of the *Asset Profile Workbook*
- *Evaluation Criteria* worksheet 3.2
- *Threat and Risk Profiles* section of the *Asset Profile Workbook*

1. Select a critical asset. Turn to the *Impact Descriptions* section of the *Asset Profile Workbook*. The section contains a table for each of four threat outcomes (disclosure, modification, destruction/loss, interruption). During activity A3.1, you added narrative descriptions for the impacts to the tables.
2. Review the impact descriptions listed in the tables. For each impact description listed in the table, evaluate it and assign it an impact measure (high, medium, or low). Use the qualitative evaluation criteria that you created during the previous activity (see the *Evaluation Criteria* worksheet 3.2). Remember to use the evaluation criteria as the benchmark against which you evaluate each impact.

   When you come to a consensus on the impact value for each impact description, write it in the appropriate table in the *Impact Descriptions* section of the workbook. Evaluate all of the impacts for a critical asset.

   Record the impact value in the *Threat and Risk Profiles* section of the *Asset Profile Workbook* in the impact column. Make sure that the impact value is recorded next to the outcome from which it was derived.
3. If there is more than one value for the impacts associated with any outcome, record all of them in the impact column. For example, if disclosure has three statements describing the impact to the organization (one with a value of "high" and two with values of "medium"), record "medium, high" in the impact column.

Additional Guidance

If you have difficulty using the evaluation criteria as you evaluate the impact descriptions, then one of the following might be occurring:

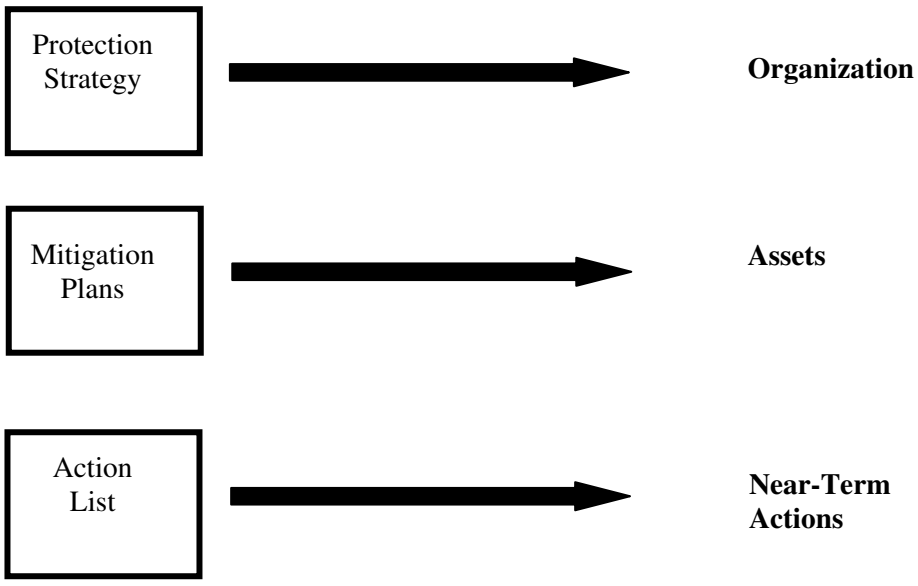
- The evaluation criteria might not be specific enough to enable you to assign measures to impact descriptions. In this case, you need to refine the evaluation criteria by making them more specific.
- The impact description might be too vague to enable you to assign measures. In this case, you need to refine the impact descriptions by making them more specific.

In the first case, you will find yourself refining the evaluation criteria.

A3.4 – A3.6	**Strategy Planning Introduction**

Basic Guidance

The diagram below illustrates the primary focus of the outputs of Risk Methodology K-12.



A protection strategy defines the strategies that an organization uses to enable, initiate, implement, and maintain its internal security. Note that the focus of the protection strategy is the organization. A protection strategy tends to be long-term, organization-wide initiatives. During the risk methodology activities, you will create a protection strategy. After completing the methodology, someone from your organization will need to generate implementation details to implement the strategy.

Risk mitigation plans are intended to reduce the risks to critical assets. Note that the focus of mitigation plans is assets. Mitigation plans include mostly mid-term actions. During the risk methodology activities, you will create risk mitigation plans. Afterward, someone from your organization will need to generate implementation details to implement each of the plans.

An action list addresses near-term actions. The action items on the list are consistent with the protection strategy and mitigation plans. They generally do not take specialized knowledge or require changes in policy to implement, and they can be implemented quickly. Thus, action items don't require the implementation details that a protection strategy or a mitigation plan requires.

Note that there is no hierarchical relationship between the protection strategy and the mitigation plans. The mitigation plans are generally consistent with the protection strategy since they are both based on security practices (and there might be some overlap between them). However, mitigation plans are not plans to implement the protection strategy. The protection strategy is focused on organizational improvement, while the mitigation plans are focused on protecting critical assets. Again, both the protection strategy and mitigation plans require implementation details to be developed after completion of the risk evaluation.

A3-4	Create Mitigation Plans	
Worksheets Used in this Activity • *Security Practices Summary* worksheet 1.7 • *Asset Profile Workbook* for each critical asset	**Outputs of this Activity** • proposed mitigation plan	**Activity Time** Use one asset

Basic Guidance

During this activity, you will be working as team to create risk mitigation plans for your critical assets. You can use any materials that will help you in your decision making. Some suggestions are

- *Current Security Practices* survey information
- *Security Requirements for Critical Assets* section of the *Asset Profile Workbook*
- *Threat and Risk Profiles* section of the *Asset Profile Workbook*
- *Areas of Concern* section of the *Asset Profile Workbook*

A mitigation plan defines the activities required to mitigate the risks/threats to the critical assets. A mitigation plan focuses on activities to

- recognize or detect threats as they occur
- resist or prevent threats from occurring
- recover from threats if they occur

1. Select a critical asset. Turn to the *Mitigation Plans* section of the asset's *Asset Profile Workbook.* There are four tables in this section, one for each of the following threat categories:
   - human actors using network access
   - human actors using physical access
   - system problems
   - other problems

   Note that the "other problems" threat category includes any additional, or custom, threat sources that you defined during Phase 1.

A3-4 Create Mitigation Plans

Basic Guidance (cont.)

2. Review the risk profile, security requirements, and areas of concern for the critical asset before developing the mitigation plan. They are found in the following sections of the workbook:
    - *Security Requirements for Critical Assets*
    - *Threat and Risk Profiles*
    - *Areas of Concern*
3. Select a threat category for the critical asset. The table for each threat category in the *Mitigation Plans* section contains the following questions for you to consider as you identify mitigation activities:
    - What actions could you take to recognize or detect this threat type as it is occurring?
    - What actions could you take to resist or prevent this threat type from occurring?
    - What actions could you take to recover from this threat type if it occurs?
    - What other actions could you take to address this threat type?
    - How will you test or verify that this mitigation plan works and is effective?
4. Develop mitigation actions for the chosen threat category. As you consider the questions for developing the mitigation plan, think about the administrative, physical, and technical practices that you could implement to mitigate the risks to the critical asset. When you come to a consensus on the mitigation practices, the scribe will record them on the worksheet. Complete mitigation plans for all of the threat categories that affect the critical asset. (Remember that not all threat categories apply to all critical assets.)
5. Move on to the next critical asset. Continue with this activity until you have completed mitigation plans for all of the critical assets and have recorded them in the appropriate *Asset Profile Workbook*.
6. As you develop the risk mitigation plans, you should think about any near-term actions that could help you develop or implement the plans. Make sure that you capture any action items that are identified as you develop mitigation plans. You will formally document your action items later in this workshop. Note any action items on a flip chart or on a piece of paper when they are identified.
7. Mitigation activities may vary by the role of the actor involved. Consider variations or responses that may be required. Note specific actor issues within the description of the mitigation plan.

A3-5	Create Action List	
Worksheets Used in this Activity	**Outputs of this Activity**	**Training**
• *Action List* worksheet W3.1	• proposed action list	Focus on one critical asset

Basic Guidance

During this activity, you will be create an action list.

An action list defines any actions that people in your organization can take in the near term without the need for specialized training, policy changes, etc. It is essentially a list of action items. As you created the protection strategy and risk mitigation plans, you should have recorded any near-term actions that could help you develop or implement the strategy and plans.

Examples of actions that can be placed on the action list include the following:

- An IT staff member can be assigned an action to fix the high-severity vulnerabilities that were identified during Phase 2.
- The analysis team and the organization's management can be assigned an action to define the details of implementing the protection strategy.

1. Review the action items that were recorded on a flip chart or on a piece of paper during this workshop. Decide if any are appropriate for the action list.

   When you come to a consensus, the scribe should record them on the *Action List* worksheet W3.1.

2. You should also think of additional near-term actions that could help you to implement your strategy and plans. Consider the following questions as you think about action items:

   - What near-term actions need to be taken?
   - Who will be responsible for the actions?
   - By when do the actions need to be addressed?
   - Does management need to take any actions to facilitate this activity?

   Record agreed actions on the *Action List* worksheet.

A3.6	Create Protection Strategy	
Worksheets Used in this Activity • *Protection Strategy Worksheet* W1.6 • *Security Practices Summary* Worksheet 1.7 • *Asset Profile Workbook* for each critical asset • *Protection Strategy Worksheets* (W3.3, W3.4, W3.5)	**Outputs of this Activity** • proposed protection strategy	**Training**

Basic Guidance

During this activity, you will be working as a team to create a proposed protection strategy for your organization. You can use any materials that will help you in your decision making. Some suggestions are

- *Protection Strategy Worksheet* W1.6
- *Security Practices Summary* Worksheet 1.7
- *Asset Profile Workbook* for each critical asset
- *Security Requirements for Critical Assets* section of the *Asset Profile Workbook*
- *Threat and Risk Profiles* section of the *Asset Profile Workbook*
- *Areas of Concern* section of the *Asset Profile Workbook*
- *Protection Strategy Worksheets* W3.3, W3.4, W3.5

During this activity, you will develop a strategy to maintain the good practices that your organization currently uses and to address organizational vulnerabilities.

A protection strategy defines the strategies that an organization uses to enable, initiate, implement, and maintain its internal security. A protection strategy focuses on organizational issues. Later in this workshop, you will create risk mitigation plans. The risk mitigation plans focus directly on reducing the risks to your critical assets. The mitigation plans have a more operational focus than the protection strategy.

The protection strategy will address strategic practices that could be used by your organization.

A3.6 Create Protection Strategy

Basic Guidance (cont.)

The protection strategy is structured around the catalog of practices, and it addresses the following areas:

- Security Awareness and Training
- Security Strategy
- Security Management
- Security Policies and Regulations
- Collaborative Security Management
- Contingency Planning/Disaster Recovery
- Physical Security
- Information Technology Security
- Staff Security

1. You will develop the strategy in two parts. First, you will develop the strategy for the following areas using the *Protection Strategy for Strategic Practices* worksheet W3.3:
   - Security Awareness and Training
   - Security Strategy
   - Security Management
   - Security Policies and Regulations
   - Collaborative Security Management
   - Contingency Planning/Disaster Recovery

   For each area, the worksheet will prompt you for the following:
   - the current practices in this area that your organization should continue to use
   - new practices that your organization should adopt

   The worksheet also provides a number of questions in each area for you to consider as you create the strategy. The questions are based on the practices that are part of the catalog of practices.

   Develop a strategy using the *Protection Strategy for Strategic Practices* worksheet. When you come to a consensus on the strategy for each area, record the strategy for the area on the worksheet.

A3.6 Create Protection Strategy

Basic Guidance (cont.)

2. Next, you will develop the strategy for the following areas using the *Protection Strategy for Operational Practices* worksheet (W3.4):

    - Physical Security
    - Information Technology Security
    - Staff Security

    When you develop this part of the protection strategy, you will consider strategies that will enable your organization to implement the operational practices from these areas. This worksheet provides questions for you to consider, focusing on the following strategies:

    - training and education initiatives
    - funding
    - policies and procedures
    - roles and responsibilities
    - collaborating with other organizations and with external experts

    Consider the questions on the worksheet as you develop the strategy for each area. When you come to a consensus on the strategy for each area, record the strategy for the area on the worksheet.

3. Finally, you will develop the strategy for the following areas using the *Protection Strategy for Educational Practices* (W3.5):

    - Content Blocking
    - Structured Access Management
    - Regulatory Compliance
    - Acceptable Use

    Consider the questions on the worksheet for each area as you develop the strategy. When you come to a consensus on the strategy for each area, record the strategy for the area on the worksheet.

4. As you develop the protection strategy, you should think about any near-term actions that could help you develop or implement your protection strategy. Make sure that you capture any action items that are identified as you develop the strategy. You will formally document your action items later in this workshop. The scribe should record any action items on a flip chart or on a piece of paper when they are identified.

A3.6 Create Protection Strategy

Additional Guidance

The *Protection Strategy for Strategic Practices* worksheet, the *Protection Strategy for Operational Practices* worksheet and the *Protection Strategy for Educational Practices* are based on a known catalog of good practice.

When you develop your protection strategy, always use your best judgment. Take into consideration the following pieces of information:

- survey results across all organizational levels
- contextual information (protection strategy practices and organizational vulnerabilities across all organizational levels)

However, you are likely to find that there will be discrepancies in the survey results across the different organizational levels. You will also find contradictions in the protection strategy practices and organizational vulnerabilities. You might even find that the survey results from an organizational level contradict the contextual information from the same level.

Your task is to make sense of the information. The core analysis team should have been present for all of the workshops, which has allowed you to hear a variety of perspectives on what is happening in the organization. Now, you have to sort through everything that you have recorded and heard during the previous workshops.

Risk Methodology K-12

Worksheets

Process Worksheets

Worksheets apply to a range of assets. For the specific details of an individual asset, use the Profile Workbook.

Worksheet Contents

Asset Worksheet

Assets
1. What are your important assets? *Consider:* • *information* • *systems* • *software* • *hardware* • *people*
2. Are there any other assets that you are required to protect (e.g., by law or regulation)?
3. What related assets are important? *Consider:* • *information* • *systems* • *software* • *hardware* • *people*
4. From the assets that you have identified, which are the most important? What is your rationale for selecting these assets as important?

Areas of Concern Worksheet

What scenarios threaten your important assets?

Sources of Threat

Deliberate Actions by People
Consider:
- *people inside your organization*
- *people outside your organization*

Accidental Actions by People
Consider:
- *people inside your organization*
- *people outside your organization*
- *yourself*

System Problems
Consider:
- *hardware defects*
- *software defects*
- *unavailability of related systems*
- *malicious code (virus, worm, Trojan horse, back door)*
- *other*

Other Problems
Consider:
- *power outages*
- *water unavailable*
- *telecommunications unavailable*
- *ISP unavailable*
- *floods*
- *earthquakes*
- *other*

Asset

Outcomes

***Disclosure* or *viewing* of sensitive information**

***Modification* of important or sensitive information**

***Destruction* or *loss* of important information, hardware, or software**

***Interruption* of access to important information, software applications, or services (email, Web, etc.)**

Current General Security Practices Survey

Current General Security Practices Survey			
Practice	**How is this practice used by your organization?**		
Security Awareness and Training			
All technology users understand their security roles and responsibilities.	Yes	No	Unknown
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation.	Yes	No	Unknown
Security awareness, training, and periodic reminders are provided for all technology users.	Yes	No	Unknown
Technology user's understanding of security information is documented and conformance is periodically verified.	Yes	No	Unknown
Security Strategy			
The organization's planning process routinely incorporate security considerations.	Yes	No	Unknown
Security strategies and policies take into consideration the organization's mission, strategies and goals.	Yes	No	Unknown
Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to all members of the organization (at least annually).	Yes	No	Unknown
Security Management			
Management allocates sufficient funds and resources to information security activities.	Yes	No	Unknown

Current General Security Practices Survey (cont.)	
Practice	**Is this practice used by your organization?**
Security Management (cont.)	
Security roles and responsibilities are defined for all personnel in the organization.	Yes No Unknown
The organization's hiring and termination practices for personnel take information security issues into account.	Yes No Unknown
The organization manages information security risks, including • assessing risks to information security • taking steps to mitigate information security risks	Yes No Unknown
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk and vulnerability assessments).	Yes No Unknown
Security Policies and Regulations	
The organization has a comprehensive set of documented, current security policies that are periodically reviewed and updated.	Yes No Unknown
There is a documented process for management of security policies, including • creation • administration (including periodic reviews and updates) • communication	Yes No Unknown
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	Yes No Unknown
The organization uniformly enforces its security policies.	Yes No Unknown

Current General Security Practices Survey (cont.)	
Practice	**Is this practice used by your organization?**
Collaborative Security Management	
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including • protecting information belonging to other organizations • understanding the security polices and procedures of external organizations • ending access to information by terminated external personnel	Yes No Unknown
The organization has verified that outsourced security services, mechanisms, and technologies meet its security needs and requirements.	Yes No Unknown
Contingency Planning/Disaster Recovery	
An analysis of operations, applications, and data criticality has been performed.	Yes No Unknown
The organization has documented, reviewed, and tested • business continuity or emergency operation plans • disaster recovery plan(s) • contingency plan(s) for responding to emergencies	Yes No Unknown
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	Yes No Unknown
All personnel needed to participate are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities	Yes No Unknown

Current General Security Practices Survey (cont.)	
Practice	**Is this practice used by your organization?**
Physical Security Plans and Procedures	
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	Yes No Unknown
There are documented policies and procedures for managing visitors.	Yes No Unknown
There are documented policies and procedures for physical control of hardware and software.	Yes No Unknown
Physical Access Control	
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Yes No Unknown
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	Yes No Unknown
System and Network Management	
There are documented and tested security plan(s) for safeguarding the systems and networks.	Yes No Unknown
There is a documented and tested data backup plan for both software and data. All personnel required to participate understand their responsibilities under the plans.	Yes No Unknown

Current General Security Practices Survey (cont.)	
Practice	**Is this practice used by your organization?**
Authentication and Authorization	
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes No Unknown
Individuals and groups are uniquely identified for tracking and monitoring purposes within the network and systems.	Yes No Unknown
Establishing and terminating the right of access for both individuals and groups is performed in a timely manner.	Yes No Unknown
Incident Management	
Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Yes No Unknown
Incident management procedures are periodically tested, verified, and updated.	Yes No Unknown
There are documented policies and procedures for working with law enforcement agencies.	Yes No Unknown

Current General Security Practices Survey (cont.)	
Practice	**Is this practice used by your organization?**
General Staff Practices	
All technology participants follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Yes No Unknown
There are documented procedures for authorizing and overseeing all personnel (including individuals from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Yes No Unknown
All staff at all levels of responsibility implements their assigned roles and responsibility for information security.	Yes No Unknown

Current Educational Security Practices Survey

Current Educational Security Practices Survey	
Practice	**How is this practice used by your organization?**
Content Blocking	
Policies and procedures for applying content blocking have been defined and installed software and hardware filtering tools are set up to implement the policy.	Yes No Unknown
Content blocking is applied appropriately to all available services (Internet, email, chat services, and applications) and all types of communication mechanisms available within the organization (desktop, laptop, PDA, wireless, cell phone, remote devices of varying kinds, etc.) based on policy which may vary by role and student age level.	Yes No Unknown
A reporting and correction capability exists for problems with content blocking. Default settings for filtering can be adjusted to correct problems. The responsibilities for problem identification and problem correction have been assigned within the organization.	Yes No Unknown
Content blocking policies and procedures are in accordance with parental and local definitions of inappropriate content (Internet sites, spam, ads, solicitations, etc.).	Yes No Unknown
Digital content used for education is evaluated for validity and appropriateness to assure learning is not jeopardized through the use of online content instead of textbooks. This process is consistently applied to all learning materials.	Yes No Unknown
Content blocking mechanisms are sufficiently supported to maintain a consistency as online content and capabilities expand.	Yes No Unknown
Purchase arrangements for technology which include vendor monitoring are evaluated for consistency with content blocking policies and procedures.	Yes No Unknown

Current Educational Security Practices Survey (cont.)	
Practice	**How is this practice used by your organization?**
Structured Access Management	
Technology choices are matched to the needs of the technology participants.	Yes No Unknown
Mechanisms have been established to assure that individuals sharing equipment cannot infringe on the privacy of others using the same equipment.	Yes No Unknown
Shared content is available through the use of bookmark files, portals and other structures that assure consistency without reliance on specific access devices.	Yes No Unknown
Policies and procedures for remote access to information are established and consistently managed. These include security considerations appropriate to the devices and applications involved.	Yes No Unknown
Technology access and availability is consistent with organizational policies for compliance with Americans with Disabilities Act.	Yes No Unknown
Software and equipment selection processes include consideration for physical and online security throughout the useful life of the purchase.	Yes No Unknown
Implementers and monitors are aware of control mechanisms (physical and online) and mechanisms exist for identification, reporting, and correction of problems throughout the useful life of the technology.	Yes No Unknown
Regulatory Compliance - COPPA	
Controls are in place to assure all private information for children under the age of 13 is not released without parental consent.	Yes No Unknown
Monitoring mechanisms are in place to assure that children cannot reach sites that do not appropriately apply COPPA restrictions in collecting information.	Yes No Unknown

Current Educational Security Practices Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Regulatory Compliance – COPPA (cont)			
Safe-harbor status has been established internally and sites approved as such have been identified for use by children under the age of 13.	Yes	No	Unknown
Regulatory Compliance – Copyright and Licensing Laws			
Appropriate use of digital materials is actively encouraged.	Yes	No	Unknown
Discussions of ethical behavior and definition of appropriate use occur on a regular basis at all levels of technology participants.	Yes	No	Unknown
Penalties for inappropriate behavior are understood as required by all levels of technology participants. Monitoring mechanisms are appropriately established.	Yes	No	Unknown
Validation mechanisms have been identified and are periodically applied to digital content to confirm appropriate licensing management.	Yes	No	Unknown
Regulatory Compliance – Federal and State Reporting			
Information collection to support mandated Federal reporting is defined and consistent with organization policies of privacy.	Yes	No	Unknown
Information distribution in handled in compliance with the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA)	Yes	No	Unknown
Compliance requirements linked to standards, assessments, curricula, teacher preparation, and professional development are consistent with organizational policies and good practices for secure use and availability.	Yes	No	Unknown
Programs to insert technology into the organization provide clear consideration for organizational policies and good practices for secure use and availability	Yes	No	Unknown

Current Educational Security Practices Survey (cont.)			
Practice	**Is this practice used by your organization?**		
Regulatory Compliance – USA PATRIOTS ACT			
Technology users are aware of the restrictions to external sites imposed by the USA PARTIOTS ACT and organizational use policy provides a means for enforcing these restrictions.	Yes	No	Unknown
Mechanisms are in place for identification of inappropriate use of organization facilities with respect to generating potential harm to other sites and the capability to identify violators and impose penalties on their actions is in place.	Yes	No	Unknown
Standards of conduct for individuals with technical skills and system access that would allow them to violate restrictions of the USA PARTIOTS ACT are clearly defined and enforced.	Yes	No	Unknown
Acceptable Use Management			
Acceptable use of all educational equipment and services is carefully defined for all technology participants.	Yes	No	Unknown
All technology participants exhibit an understanding of the required policies and procedures for use of educational technology.	Yes	No	Unknown
External groups such as parents, school boards, and other influential local organizations are clearly aware of the acceptable use of educational equipment and services and support the organization in its implementation.	Yes	No	Unknown
The appropriate use of technology in meeting the goals of the organization is clearly defined and applied by all decision makers.	Yes	No	Unknown

Current Educational Security Practices Survey (cont.)	
Practice	**Is this practice used by your organization?**
Acceptable Use Management (cont.)	
Penalties for inappropriate use are clearly defined and understood by all technology participants.	Yes No Unknown
The use and responsibilities for participants in special programs with technology components have been clearly defined and communicated to all participants.	Yes No Unknown
Acceptable use includes communication of the risks of technology use to participants. These have been appropriately defined and communicated to all participants (teachers, students, parents).	Yes No Unknown
A process monitoring acceptable use has been defined and implemented. This includes a means for participants to report problems and threats conveyed through the technology.	Yes No Unknown
Licensing restrictions and other limitations for the use of technology are clearly communicated to all participants.	Yes No Unknown
Mechanisms have been established to identify unacceptable use and link it to the appropriate individual for evaluation and application of penalties.	Yes No Unknown

Current IT Security Practices Survey

Current IT Security Practices Survey	
Practice	**How is this practice used by your organization?**
Security Awareness and Training	
Technology selection is linked to the mission of the organization and includes consideration of security issues.	Yes No Unknown
Security Management	
Visibility of machines to external probes is managed such that no private data (including location) can be identified.	Yes No Unknown
Protections are applied so that collection facilities such as cookies, doubleclick modules, and other options invisible to the user are limited to public information.	Yes No Unknown
Security Policies and Regulations	
Policies that identify restrictions to access (e.g. Internet entertainment) include consideration for the limitations of technology and resource requirements for implementation.	Yes No Unknown
Monitoring and Auditing Physical Security	
Maintenance records are kept to document the repairs and modifications of a facility's physical components.	Yes No Unknown
An individual's or group's actions, with respect to all physically controlled media, can be accounted for.	Yes No Unknown
Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.	Yes No Unknown

Current IT Security Practices Survey (cont)	
Practice	**How is this practice used by your organization?**
System and Network Management	
Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information).	Yes No Unknown
The integrity of installed software is regularly verified.	Yes No Unknown
All systems are up to date and with respect to revisions, patches, and recommendations in security advisories.	Yes No Unknown
Changes to IT hardware and software are planned, controlled, and documented.	Yes No Unknown
IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. • Unique user identification is required for all information system users, including third-party users. • Default accounts and default passwords have been removed from systems.	Yes No Unknown
Only necessary services are running on systems – all unnecessary services have been removed.	Yes No Unknown
System Administration Tools	
Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.	Yes No Unknown

Current IT Security Practices Survey (cont)	
Practice	**How is this practice used by your organization?**
Monitoring and Auditing IT Security	
System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.	Yes No Unknown
Firewall and other security components are periodically audited for compliance with policy.	Yes No Unknown
Authentication and Authorization	
Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.	Yes No Unknown
Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.	Yes No Unknown
Security Architecture and Design	
System architecture and design for new and revised systems include considerations for • security strategies, policies, and procedures • history of security compromises • results of security risk assessments	Yes No Unknown
The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.	Yes No Unknown

Current IT Security Practices Survey (cont)	
Practice	**How is this practice used by your organization?**
Vulnerability Management	
There is a documented set of procedures for managing vulnerabilities, including • selecting vulnerability evaluation tools, checklists, and scripts • keeping up to date with known vulnerability types and attack methods • reviewing sources of information on vulnerability announcements, security alerts, and notices • identifying infrastructure components to be evaluated • scheduling of vulnerability evaluations • interpreting and responding to the results • maintaining secure storage and disposition of vulnerability data	Yes No Unknown
Vulnerability management procedures are followed and are periodically reviewed and updated.	Yes No Unknown
Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.	Yes No Unknown
Encryption	
Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).	Yes No Unknown
Encrypted protocols are used when remotely managing systems, routers, and firewalls.	Yes No Unknown

Protection Strategy Worksheet

Protection Strategy
1. Which issues from the survey would you like to discuss in more detail?
2. What important issues did the survey not cover?
3. Are there specific security policies, procedures, and practices unique to certain assets? What are they?
4. Do you think that your organization's protection strategy is effective? How do you know?

Security Practices Summary

Based on responses to the surveys, summarize the results in the following tables:

Summary of General Security Practices

Practice Area	Status		
Security Awareness and Training	Fine	Needs Improvement	Needs Research
Security Strategy	Fine	Needs Improvement	Needs Research
Security Management	Fine	Needs Improvement	Needs Research
Security Policies and Regulations	Fine	Needs Improvement	Needs Research
Collaborative Security Management	Fine	Needs Improvement	Needs Research
Contingency Planning/Disaster Recovery	Fine	Needs Improvement	Needs Research
Physical Security Plans and Procedures	Fine	Needs Improvement	Needs Research
Physical Access Control	Fine	Needs Improvement	Needs Research
System and Network Management	Fine	Needs Improvement	Needs Research
Authentication and Authorization	Fine	Needs Improvement	Needs Research
Incident Management	Fine	Needs Improvement	Needs Research
General Staff Practices	Fine	Needs Improvement	Needs Research

Summary of Educational Security Practices

Practice Area	Status		
Content Blocking	Fine	Needs Improvement	Needs Research
Structured Access Management	Fine	Needs Improvement	Needs Research
Regulatory Compliance - COPPA	Fine	Needs Improvement	Needs Research
Regulatory Compliance – Copyright and Licensing Laws	Fine	Needs Improvement	Needs Research
Regulatory Compliance – Federal and State Reporting	Fine	Needs Improvement	Needs Research
Regulatory Compliance – USA PARTIOTS ACT	Fine	Needs Improvement	Needs Research
Acceptable Use Management	Fine	Needs Improvement	Needs Research

Security Practices Summary (cont)

Summary of IT Security Practices

Practice Area	Status		
Security Awareness and Training	Fine	Needs Improvement	Needs Research
Security Management	Fine	Needs Improvement	Needs Research
Security Policies and Regulations	Fine	Needs Improvement	Needs Research
Monitoring and Auditing Physical Security	Fine	Needs Improvement	Needs Research
System and Network Management	Fine	Needs Improvement	Needs Research
System Administration Tools	Fine	Needs Improvement	Needs Research
Monitoring and Auditing IT Security	Fine	Needs Improvement	Needs Research
Authentication and Authorization	Fine	Needs Improvement	Needs Research
Security Architecture and Design	Fine	Needs Improvement	Needs Research
Vulnerability Management	Fine	Needs Improvement	Needs Research
Encryption	Fine	Needs Improvement	Needs Research

Identify Evaluation Criteria

Organizational Measurements
1. What criteria are used to define success or failure of projects? • regulatory compliance • classroom plans and curriculum effectiveness • life/health/safety of students, teachers, and staff • student performance on standardized tests and evaluations • family and community support • school and district administration support • teacher preparation • other
2. How are the criteria measured? • Regulatory reporting • Budget allocations • Standardized tests • Insurance • Special reports • Formal complaints from parents, teachers, or students • Other

Organizational Measurements
3. Do the measurement criteria change if the considerations are administrative, teaching, or learning focused?
4. Should the criteria be discussed with other groups in the organization?

Action List Worksheet

Action Item	**Information**
	responsibility: *completion date:* *required management actions:*
	responsibility: *completion date:* *required management actions:*

Action Item	Information
	responsibility: *completion date:* *required management actions:*
	responsibility: *completion date:* *required management actions:*

Evaluation Criteria			
Impact Area	**High**	**Medium**	**Low**
Regulatory Compliance			
Classroom plans and curriculum effectiveness			

Evaluation Criteria			
Impact Area	**High**	**Medium**	**Low**
Life, Health, and Safety of Students, Teachers, Staff			
Student Performance on Standardized Tests and Evaluations			
Family and Community Support			

Evaluation Criteria			
Impact Area	**High**	**Medium**	**Low**
School and District Administration Support			
Teacher Preparation			
Other			

Protection Strategy For Strategic Practices (W3.3)

Protection Strategy for Strategic Practices Security Awareness and Training (SP1)	
Questions to Consider	**Strategies**
• What can you do to maintain or improve the level of information security training that all staff members receive (consider awareness training as well as technology-related training)? • Does your organization have adequate in-house expertise for all supported technologies? What can you do to improve your staff's technology expertise? • What can you do to ensure that all staff members understand their security roles and responsibilities?	*Consider:* • *The current strategies in this area that your organization should continue to use* • *New strategies that your organization should adopt*
Issues: What issues related to security awareness and training cannot be addressed by your organization?	

Protection Strategy for Strategic Practices Security Strategy (SP2)	
Questions to Consider	**Strategies**
• Are security issues incorporated into your organization's planning process? What can you do to improve the way in which security issues are integrated with your organization's strategy? • Are other organizational issues incorporated into your organization's security strategy? What can you do to improve the way in which all planning issues are integrated with your organization's security strategy? • What can you do to improve the way in which security strategies, goals, and objectives are documented and communicated to the organization?	*Consider:* • *The current strategies in this area that your organization should continue to use* • *New strategies that your organization should adopt*
Issues: What issues related to security strategy cannot be addressed by your organization?	

Protection Strategy for Strategic Practices Security Management (SP3)	
Questions to Consider	**Strategies**
• Does management allocate sufficient funds and resources to information security activities? What level of funding for information security activities is appropriate for your organization? • What can you do to ensure that security roles and responsibilities are defined for all staff in your organization? • Do your organization's hiring and retention practices take information security issues into account (also applies to contractors and vendors)? What could you do to improve your organization's hiring and retention practices? • What can you do to improve the way in which your organization manages its information security risk? • What can you do to improve the in which security-related information is communicated to your organization's management?	*Consider:* • *The current strategies in this area that your organization should continue to use* • *New strategies that your organization should adopt*
Issues: What issues related to security management cannot be addressed by your organization?	

Protection Strategy for Strategic Practices Security Policies and Regulations (SP4)	
Questions to Consider	**Strategies**
• What can you do to ensure that your organization has a comprehensive set of documented, current security policies? • What can you do to improve the way in which your organization creates, updates, and communicates security policies? • Does your organization have procedures to ensure compliance with laws and regulations affecting security? What can you do to improve how well your organization complies with laws and regulations affecting security? • What can you do to ensure that your organization uniformly enforces its security policies?	*Consider:* • *The current strategies in this area that your organization should continue to use* • *New strategies that your organization should adopt*
Issues: What issues related to security policies and regulations cannot be addressed by your organization?	

Protection Strategy for Strategic Practices Collaborative Security Management (SP5)	
Questions to Consider	**Strategies**
• Does your organization have policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners)? What can your organization do to improve the way in which it protects information when working with external organizations? • What can your organization do to improve the way in which it verifies that external organizations are taking proper steps to protect critical information and systems? • What can your organization do to improve the way in which it verifies that outsourced security services, mechanisms, and technologies meet its needs and requirements?	*Consider:* • *The current strategies in this area that your organization should continue to use* • *New strategies that your organization should adopt*
Issues: What issues related to collaborative security management cannot be addressed by your organization?	

Protection Strategy for Strategic Practices

Contingency Planning/Disaster Recovery (SP6)

Questions to Consider	Strategies
• Does your organization have a defined business continuity plan? Has the business continuity plan been tested? What can you do to ensure that your organization has a defined and tested business continuity plan? • Does your organization have a defined disaster recovery plan? Has the disaster recovery plan been tested? What can you do to ensure that your organization has a defined and tested disaster recovery plan? • What can you do to ensure that staff members are aware of and understand your organization's business continuity and disaster recovery plans?	*Consider:* • *The current strategies in this area that your organization should continue to use* • *New strategies that your organization should adopt*

Issues: What issues related to contingency planning and disaster recovery cannot be addressed by your organization?

Protection Strategy For Operational Practices Worksheet

Protection Strategy for Operational Practices Physical Security (OP1)	
Questions to Consider	**Strategies**
• What training and education initiatives could help your organization maintain or improve its physical security practices? • What funding level is appropriate to support your organization's physical security needs? • Are your policies and procedures sufficient for your organization's physical security needs? How could they be improved? • Who has responsibility for physical security? Should anyone else be involved? • What other departments in your organization should be involved with physical security? • What external experts could help you with physical security? How will you communicate your requirements? How will you verify that your requirements were met?	
Issues: What issues related to physical security cannot be addressed by your organization?	

Protection Strategy for Operational Practices Information Technology Security (OP2)	
Questions to Consider	**Strategies**
• What training and education initiatives could help your organization maintain or improve its information technology security practices? • What funding level is appropriate to support your organization's information technology security needs? • Are your policies and procedures sufficient for your organization's information technology security needs? How could they be improved? • Who has responsibility for information technology security? Should anyone else be involved? • What other departments in your organization should be involved with information technology security? • What external experts could help you with information technology security? How will you communicate your requirements? How will you verify that your requirements were met?	
Issues: What issues related to information technology security cannot be addressed by your organization?	

Protection Strategy for Operational Practices Staff Security (OP3)	
Questions to Consider	**Strategies**
• What training and education initiatives could help your organization maintain or improve its staff security practices? • What funding level is appropriate to support your staff security needs? • Are your policies and procedures sufficient for your staff security needs? How could they be improved? • Who has responsibility for staff security? Should anyone else be involved? • What other departments in your organization should be involved with staff security? • What external experts could help you with staff security? How will you communicate your requirements? How will you verify that your requirements were met?	
Issues: What issues related to staff security cannot be addressed by your organization?	

Protection Strategy for Educational Practices Content Blocking (ED1)	
Questions to Consider	**Strategies**
• What training and education initiatives could help your organization maintain or improve its content blocking practices? • What funding level is appropriate to support your content blocking needs? • Are your policies and procedures sufficient for your content blocking needs? How could they be improved? • Who has responsibility for defining and implementing the details of content blocking? Should anyone else be involved? • How are problems identified and addressed? Would adjustments in these procedures improve the value of content blocking? • What external experts could help you with defining and implementing content blocking? How will you communicate your requirements? How will you verify that your requirements were met?	
Issues: What issues related to content blocking cannot be addressed by your organization?	

Protection Strategy for Educational Practices Structured Access Management (ED2)	
Questions to Consider	**Strategies**
• What training and education initiatives could help your organization maintain or improve its technology selection and distribution practices? • What funding level is appropriate to support your technology infrastructure needs? • Are your policies and procedures sufficient for your technology access and availability needs? How could they be improved? • Who has responsibility for defining and implementing the decisions on availability and distribution and access control? Should anyone else be involved? • How are problems identified and addressed? Would adjustments in these procedures improve the value of technology? • What external experts could help you with defining and implementing appropriate levels of availability and access? How will you communicate your requirements? How will you verify that your requirements were met?	
Issues: What issues related to structured access management cannot be addressed by your organization?	

Protection Strategy for Educational Practices Regulatory Compliance (ED3)	
Questions to Consider	**Strategies**
• What training and education initiatives could help your organization maintain or improve its regulatory compliance practices? • What funding level is appropriate to support your regulatory compliance needs? • Are your policies and procedures sufficient for your regulatory compliance needs? How could they be improved? • Who has responsibility for defining and implementing the details of regulatory compliance? Should anyone else be involved? • How are problems identified and addressed? Would adjustments in these procedures improve the level of regulatory compliance? • What external experts could help you with defining and implementing levels of regulatory compliance? How will you communicate your requirements? How will you verify that your requirements were met?	
Issues: What issues related to regulatory compliance cannot be addressed by your organization?	

Protection Strategy for Educational Practices Acceptable Use (ED4)	
Questions to Consider	**Strategies**
• What training and education initiatives could help your organization maintain or improve its acceptable use practices? • What funding level is appropriate to support your establishing and monitoring acceptable use? • Are your policies and procedures sufficient for your acceptable use requirements? How could they be improved? • Who has responsibility for defining and implementing the details of acceptable use? Should anyone else be involved? • How are problems identified and addressed? Would adjustments in these procedures improve the compliance of acceptable use? • What external experts could help you with defining and implementing appropriate levels of acceptable use? How will you communicate your requirements? How will you verify that your requirements were met?	
Issues: What issues related to acceptable use cannot be addressed by your organization?	

Risk Methodology K-12

Asset Profile Workbook

Table of Contents
Asset Profile Workbook

AP1 Select Critical Assets

Critical Asset Information	
Asset	
Rationale for selection as a critical asset	
Brief description	
Roles accessing the asset (insiders and outsiders)	

AP2: Areas of Concern

Areas of Concern		
#	Outcome	Area of Concern (access, actor, motive)

Areas of Concern		
#	Outcome	Area of Concern (access, actor, motive)

Areas of concern		
#	Outcome	Area of Concern (access, actor, motive)

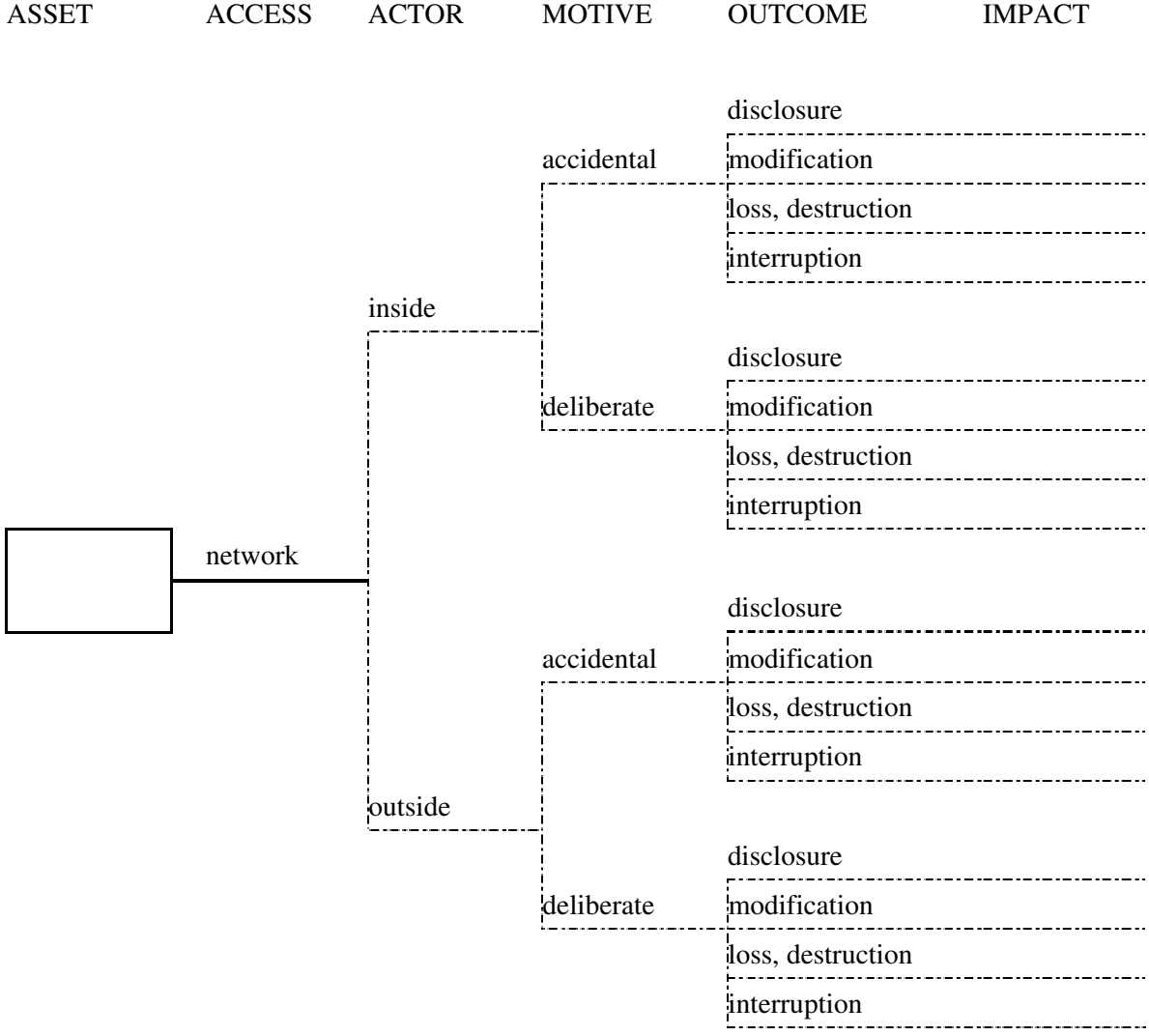
AP3 Security Requirements

Security Requirement Type	Relative Priority	Specific Requirement
Confidentiality		
Integrity		
Availability		
Other		

AP4 Threats

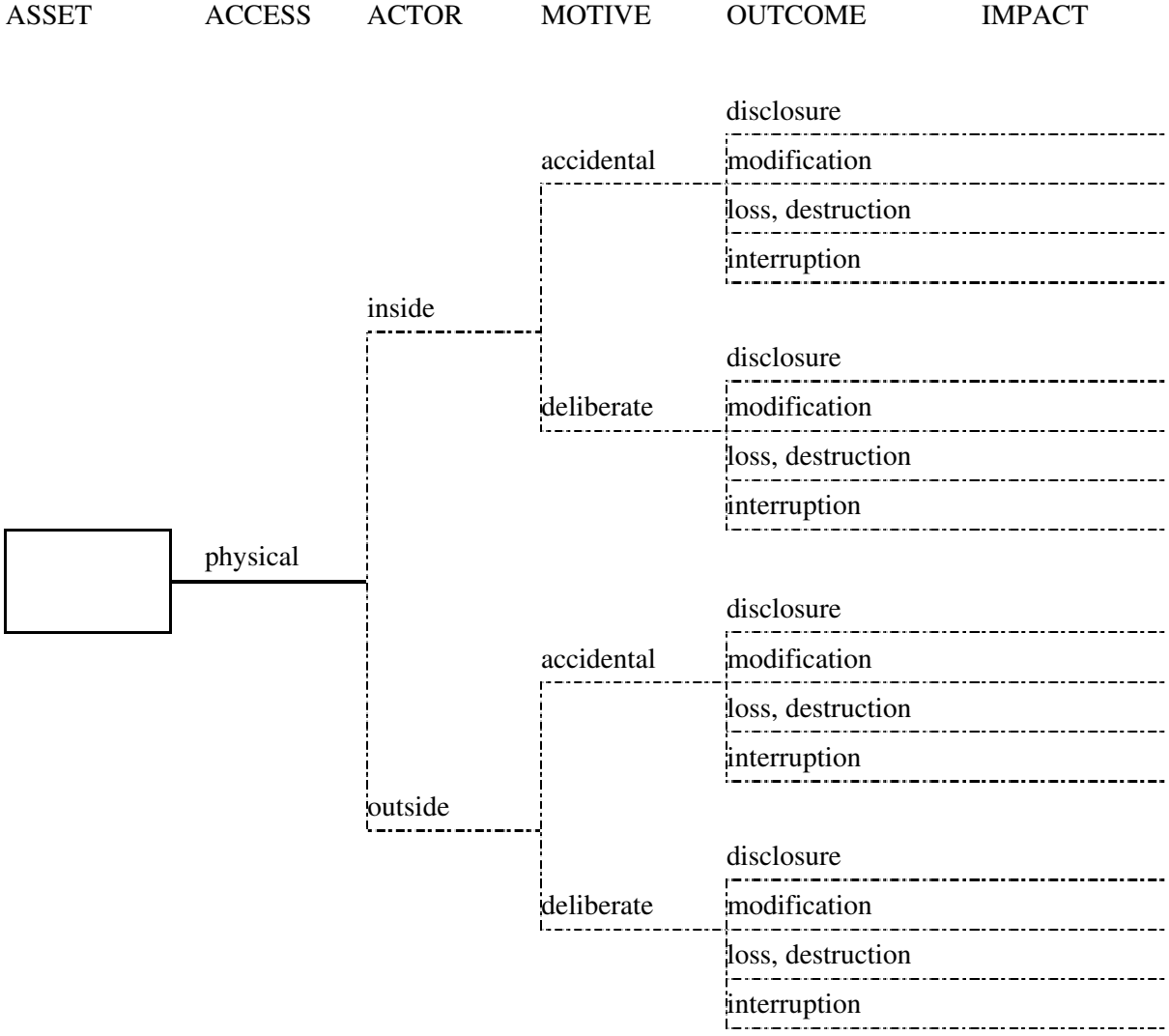
Instructions	This set of trees will be completed in two parts. First, all branches of the trees up to **but not including** "Impact" are completed. Later, in the Impact Values and Risk Profiles Section (Activity A7.3), you will come back to this section and add the impact value. 1. Review the security requirements and asset information in this workbook and the areas of concern for this asset on Worksheet W4.3.
	2. Which branches correspond to an expressed area of concern? Mark these branches on the appropriate tree.
	3. Review the remaining, unmarked branches (gaps) for threats that were not identified by the participants in the earlier workshops. Consider the following: • For which of the remaining branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree. • For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.
	4. Add notes where needed to clarify threats, especially those not covered by an existing area of concern.
	5. Use the blank "Other Problems (cont.)" threat tree to add any threats not covered by these trees, modifying the tree as needed.

Human Actors Using Network Access



Note:

Human Actors Using Physical Access



Note:

System Problems

ASSET	ACTOR	OUTCOME	IMPACT
	software defects	disclosure	
		modification	
		loss, destruction	
		interruption	
	viruses	disclosure	
		modification	
		loss, destruction	
		interruption	
	system crashes	disclosure	
		modification	
		loss, destruction	
		interruption	
	hardware defects	disclosure	
		modification	
		loss, destruction	
		interruption	

Note:

Other Problems

ASSET	ACTOR	OUTCOME	IMPACT
	power supply problems	disclosure	
		modification	
		loss, destruction	
		interruption	
	telecommunications problems or unavailability	disclosure	
		modification	
		loss, destruction	
		interruption	
	third-party problems or unavailability of third-party systems	disclosure	
		modification	
		loss, destruction	
		interruption	
	natural disasters (e.g., flood, fire, tornado)	disclosure	
		modification	
		loss, destruction	
		interruption	
	physical configuration or arrangement of buildings, offices, or equipment	disclosure	
		modification	
		loss, destruction	
		interruption	

Note:

Other Problems (cont.)

ASSET	ACTOR	OUTCOME	IMPACT
		disclosure	
		modification	
		loss, destruction	
		interruption	
		disclosure	
		modification	
		loss, destruction	
		interruption	
		disclosure	
		modification	
		loss, destruction	
		interruption	
		disclosure	
		modification	
		loss, destruction	
		interruption	
		disclosure	
		modification	
		loss, destruction	
		interruption	

Note:

AP5 Identify System of Interest

System(s) of interest	
Access paths to system(s) of interest	
Other related systems of concern linked to the critical asset	

AP6 Identify Key Classes of Components

Class of Component	Rationale for Selection
❑ Servers	
❑ Networking components	
❑ Security components	
❑ Desktop workstations	
❑ Home computers	
❑ Laptops	
❑ Storage devices	
❑ Wireless components	
❑ Others (list) _____ _____	

AP7 Identify Infrastructure Components to Examine

Class of Component	Selected Component/ IP Addresses/Host Names	Rationale	Approach
System of interest			
Systems/servers			

Class of Component	Selected Component/ IP Addresses/Host Names	Rationale	Approach
Networking components			
Security components			
Desktop workstations			

Class of Component	Selected Component/ IP Addresses/Host Names	Rationale	Approach
Home computers			
Laptops			
Storage devices			
Wireless components			

Class of Component	Selected Component/ IP Addresses/Host Names	Rationale	Approach
Others			

AP8 Technology Vulnerabilities Summary by Component Class

Class	Selected Component/ IP Address/Host Name	Vulnerability Summary

AP9 Actions/Recommendations for Vulnerabilities

Actions and Recommendations for Addressing Technology Vulnerabilities

AP10 Potential Organizational Impacts from Compromised Critical Asset

Potential Impacts to the Organization from Compromised Critical Asset			
Outcome	**Consider**	**Impact Descriptions**	**Values**
Disclosure	How could the organization be affected if this asset were disclosed? • Regulatory compliance failure • Loss of classroom time and curriculum effectiveness • Issues for life/health/safety of students, teachers, and staff • Student performance levels on standardized tests and evaluations • Loss of family and community support • Loss of school and district administration support • Loss for teacher preparation • Lawsuits could be filed against the organization or related groups (School Board) or Individuals (Superintendent) • Other impacts		

Potential Impacts to the Organization from Compromised Critical Asset			
Outcome	**Consider**	**Impact Descriptions**	**Values**
Modification	How could the organization be affected if this asset were modified? • Regulatory compliance failure • Loss of classroom time and curriculum effectiveness • Issues for life/health/safety of students, teachers, and staff • Student performance levels on standardized tests and evaluations • Loss of family and community support • Loss of school and district administration support • Loss for teacher preparation • Lawsuits could be filed against the organization or related groups (School Board) or Individuals (Superintendent) • Other impacts		

Potential Impacts to the Organization from Compromised Critical Asset			
Outcome	**Consider**	**Impact Descriptions**	**Values**
Destruction/ Loss	How could the organization be affected if this asset were destroyed, lost, or unavailable? • Regulatory compliance failure • Loss of classroom time and curriculum effectiveness • Issues for life/health/safety of students, teachers, and staff • Student performance levels on standardized tests and evaluations • Loss of family and community support • Loss of school and district administration support • Loss for teacher preparation • Lawsuits could be filed against the organization or related groups (School Board) or Individuals (Superintendent) • Other impacts		

Potential Impacts to the Organization from Compromised Critical Asset			
Outcome	**Consider**	**Impact Descriptions**	**Values**
Interruption	How could the organization be affected if access to this asset were unavailable? • Regulatory compliance failure • Loss of classroom time and curriculum effectiveness • Issues for life/health/safety of students, teachers, and staff • Student performance levels on standardized tests and evaluations • Loss of family and community support • Loss of school and district administration support • Loss for teacher preparation • Lawsuits could be filed against the organization or related groups (School Board) or Individuals (Superintendent) • Other impacts		

AP11 Mitigation Plans

Mitigation Plan for Human Actors Using Network Access	
Questions	**Actions**
What actions could you take to recognize or detect this threat type as it is occurring?	*Consider administrative, physical, and technical actions that you could take.*
What actions could you take to resist or prevent this threat type from occurring?	
What actions could you take to recover from this threat type if it occurs?	
What other actions could you take to address this threat type?	
How will you test or verify that this mitigation plan works and is effective?	

Mitigation Plan for Human Actors Using Physical Access	
Questions	**Actions**
What actions could you take to recognize or detect this threat type as it is occurring? What actions could you take to resist or prevent this threat type from occurring? What actions could you take to recover from this threat type if it occurs? What other actions could you take to address this threat type? How will you test or verify that this mitigation plan works and is effective?	*Consider administrative, physical, and technical actions that you could take.*

Mitigation Plan for System Problems	
Questions	**Actions**
What actions could you take to recognize or detect this threat type as it is occurring?	*Consider administrative, physical, and technical actions that you could take.*
What actions could you take to resist or prevent this threat type from occurring?	
What actions could you take to recover from this threat type if it occurs?	
What other actions could you take to address this threat type?	
How will you test or verify that this mitigation plan works and is effective?	

Mitigation Plan for Other Problems	
Questions	**Actions**
What actions could you take to recognize or detect this threat type as it is occurring? What actions could you take to resist or prevent this threat type from occurring? What actions could you take to recover from this threat type if it occurs? What other actions could you take to address this threat type? How will you test or verify that this mitigation plan works and is effective?	*Consider administrative, physical, and technical actions that you could take.*